Audit Report

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE

YEAR 2000 CONTINGENCY PLANNING AND COST REPORTING AT THE DEFENSE FINANCE AND ACCOUNTING SERVICE

Report No. 99-049

December 10, 1998

Office of the Inspector General
Department of Defense

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Year 2000 Contingency Planning and Cost Reporting at the Defense Finance and Accounting Service

B. DATE Report Downloaded From the Internet: 09/07/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/07/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

Additional Information and Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Analysis, Planning, and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932, or visit the Inspector General, DoD, web page at www.dodig.osd.mil.

Suggestions for Audits

To suggest ideas for or to request future audits, contact the Planning and Coordination Branch of the Analysis, Planning, and Technical Support Directorate at (703) 604-8908 (DSN 664-8908) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: APTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
CIO	Chief Information Officer
DCPS	Defense Civilian Pay System
DFAS	Defense Finance and Accounting Service
DLA	Defense Logistics Agency
DRAS-APS	Defense Retiree and Annuitant Pay System-Annuitant Pay Subsystem
GAO	General Accounting Office
IAPS	Integrated Accounts Payable System
IPC	Integrated Paying and Collecting System
IG	Inspector General
MOCAS	Mechanization of Contract Administration Services
OMB	Office of Management and Budget
POC	Point of Contact
SRD-1	Standard Finance System
Y2K	Year 2000

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

December 10, 1998

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Audit Report on Year 2000 Contingency Planning and Cost Reporting at The Defense Finance and Accounting Service (Report No. 99-049)

We are providing this report for your information and use. We considered management comments on a draft of this report in preparing the final report.

We issued two memorandums to Defense Finance and Accounting Service management to communicate issues identified during the audit. We received responses from the Defense Finance and Accounting Service and incorporated those comments into the draft report. Management comments on the draft report conformed to the requirements of DoD Directive 7650.3, and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Kimberley Caprio at (703) 604-9139 (DSN 664-9139), e-mail kcaprio@dodig.osd.mil, or Mr. Michael Perkins at (703) 604-9152 (DSN 664-9152), e-mail mperkins@dodig.osd.mil. See Appendix H for the report distribution. The audit team members are listed inside the back cover.

Robert J Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-049 **December 10, 1998**
(Project No. 8FG-6020)

Year 2000 Contingency Planning and Cost Reporting at the Defense Finance and Accounting Service

Executive Summary

Introduction. This is one of a series of reports being issued by the Inspector General, (IG) DoD, in an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the Year 2000 computing challenge. For a listing of audit projects addressing the issue, see the Year 2000 web page on the IGnet at www.ignet.gov.

Audit Objectives. The overall audit objective was to determine the effectiveness of the Defense Finance and Accounting Service (DFAS) initiatives for addressing the Year 2000 computer problem. For this report, we evaluated whether DFAS:

- complied with the requirements of the DoD Year 2000 Management Plan,
- prepared adequate Year 2000 system-level contingency plans, and
- reported complete and reliable Year 2000 system cost estimates to the Office of Management and Budget and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

Audit Results. DFAS has issued good corporate-level guidance for Year 2000 contingency planning; however, more needs to be done to ensure the completeness and practicality of system level contingency plans. System managers at DFAS did not establish adequate Year 2000 contingency plans. System managers for systems that DFAS shares with other agencies did not have contingency plans that adequately addressed DFAS business functions. DFAS system managers also did not complete reliable cost estimates for reporting to the Office of Management and Budget and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). DFAS has initiated actions to address the contingency planning issues (Finding A), and has emphasized cost reporting requirements to system managers (Finding B). These proposed actions, if completed, should address some of our concerns.

Summary of Recommendations. We recommend that the DFAS Director, Information and Technology, establish a verification mechanism to ensure that system managers establish contingency plans that meet the elements in the DFAS Year 2000 Contingency Planning Guidance. In addition, we recommend that contingency plans addressing the DFAS business processes be established for DFAS systems that are jointly owned.

Management Actions during Audit. Management actions were responsive to suggestions made during the review. The DFAS Director, Information and

Technology, must ensure that the agreed-on actions are completed and that the status of ongoing actions is monitored.

Management Comments. DFAS concurred with the recommendations in the draft audit report. DFAS stated that the DFAS Contingency Planning Guidance requires that Y2K Contingency Plans be reviewed and signed by the system manager, Center Director, and headquarters functional representative. Also, the DFAS Y2K Project Officer will track the completion of the required contingency plans. In addition, to ensure that DFAS jointly-owned systems have adequate contingency plans addressing the DFAS business processes, DFAS is developing Core/Core Support Business Process contingency plans. See Part I for a discussion of management comments and Part III for the full text of management comments.

Audit Response: The corrective actions by DFAS met the intent of our recommendations. Therefore, management comments are considered responsive and no further comments are required. We commend DFAS responsiveness to the issues identified by the audit.

Table of Contents

Part I - Audit Results

Introduction

This audit report, which is one in a series of reports on the Defense Finance and Accounting Service (DFAS) Year 2000 (Y2K) initiatives, discusses our review of contingency plans and cost reporting. We previously issued reports on Y2K initiatives at the DFAS Cleveland Center (see Appendix B for references to the details of the reports).

Background

DFAS is responsible for DoD finance and accounting operations and the operability of information systems used to perform these functions. Each year, DFAS pays over 3 million military and civilian personnel, 2 million retirees and annuitants, and 23 million invoices to contractors and vendors. On a monthly basis, DFAS processes more than 9.8 million payments to DoD personnel and more than 1 million payments to DoD vendors and contractors, with a monthly disbursing total exceeding $22 billion. DFAS maintains monthly reports on the Y2K status of 179 systems. The monthly report categorizes systems to be changed, replaced, or terminated, and those that are Y2K compliant. Y2K issues can affect every aspect of the DFAS finance and accounting mission because DFAS relies heavily on computer systems to carry out its operations.

Because of the potential failure of computers to run or function throughout the Government, the President issued an Executive Order, "Year 2000 Conversion," February 4, 1998, making it policy that Federal agencies ensure that no critical Federal program experiences disruption because of the Y2K problem and that the head of each agency ensure that efforts to address the Y2K problem receive the highest priority attention in the agency.

OMB Reporting Requirements. OMB is required to submit quarterly summary reports to Congress on the Administration's progress in addressing the Y2K problem. OMB issued OMB Memorandum No. 98-12, "Revised Reporting Guidance on Year 2000 Efforts," July 22, 1998, requiring quarterly reports on the status of agency efforts. Each agency is required to report on mission-critical systems, including the number of systems that are Y2K compliant, being replaced and repaired, and scheduled to be retired.

DoD Reporting Requirements. As the DoD Chief Information Officer (CIO), the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) ASD(C^3I) issued memorandums on March 12, 1997, "Y2K Refined Reporting Requirements for DoD," and on June 19, 1998, "Year 2000 Database Reporting." The memorandums establish requirements for reporting Y2K progress throughout DoD. Reports should reflect the status of DoD Y2K efforts and fulfill OMB reporting requirements.

The Secretary of Defense issued a memorandum, "Year 2000 Compliance," on August 7, 1998, and stated that DoD is making insufficient progress in its efforts

The Secretary of Defense issued a memorandum, "Year 2000 Compliance," on August 7, 1998, and stated that DoD is making insufficient progress in its efforts to solve the Y2K computer problem, which he termed a critical national defense issue. Consequently, the Defense agencies will be responsible for ensuring that the list of mission-critical systems under their purview is accurately reported in the DoD Y2K database, with each change in mission-critical designation reported and explained within 1 month of the change to the Office of the Assistant Secretary (Command, Control, Communications, and Intelligence) effective October 1, 1998.

The Deputy Secretary of Defense issued a memorandum, "Year 2000 (Y2K) Verification of National Security Capabilities," on August 24, 1998. The memorandum states that all the Directors of Defense agencies must certify that they have tested the information technology and national security system Y2K capabilities of their agencies' systems in accordance with the DoD Management Plan. The memorandum also emphasized that each Principal Staff Assistant of the Office of the Secretary of Defense must verify that all functions under his or her purview will continue unaffected by Y2K issues. For the finance and accounting functions, the Principal Staff Assistant is the Under Secretary of Defense (Comptroller).

Objective

The overall audit objective was to determine the effectiveness of DFAS initiatives to address the Y2K computer problem as DFAS systems approached the last three phases of renovation, validation, and implementation. For this report, we evaluated whether DFAS:

- complied with the requirements of the DoD Year 2000 Management Plan,
- prepared adequate Y2K system-level contingency plans, and
- reported complete and reliable Y2K system cost estimates to the OMB and the ASD(C^3I).

We did not review the management control program as it relates to the overall audit objective because DFAS and DoD identified Y2K conversion problems as an uncorrected material weakness in their Annual Statements of Assurance for FYs 1996 and 1997. See Appendix A for a discussion of the audit scope and methodology.

Finding A. Adequacy of the DFAS Contingency Plans

Although DFAS has put corporate level emphasis on Y2K contingency planning, system-level contingency plans did not adequately address methods for conducting business operations in the event of a Y2K system failure. DFAS is a joint owner when it owns less than 50 percent of a system. For these systems, DFAS did not have contingency plans that adequately addressed alternative work processes for maintaining the continuity of DFAS business functions. Contingency plans were inadequate because system managers did not have sufficient guidance for establishing contingency plans. Also, DFAS focused efforts on identifying, assessing, and changing systems affected by the Y2K problem, rather than on establishing contingency plans. If critical systems suffer Y2K-related failures, inadequate contingency plans may lengthen the amount of time that will elapse before business operations can resume.

Requirement for Contingency Plans

Purpose of Contingency Plans. A contingency plan should describe the steps an organization would take to maintain essential business processes in the event a system is degraded, unreliable, or rendered inoperable. Contingency plans allow management and operations personnel to deal with unexpected losses. For the Y2K problem, a contingency plan may involve preparing and partially implementing alternative work processes if critical systems fail unexpectedly. A Y2K contingency plan should address disruptions at interfaces, transfer of corrupt data, and failure of utilities and infrastructure. Contingency plans also define the specific conditions that will activate the plan.

General Accounting Office (GAO) Report No. AIMD-97-117 (OSD Case No. 1392), "Defense Computers: DFAS Faces Challenges in Solving the Y2K Problem," August 11, 1997. The report states that DFAS had not prepared contingency plans to be used if renovations are not completed in time or systems fail to operate properly. The report recommended that DFAS issue continuity of operations guidance. After the report was issued, DFAS took action on the GAO concerns and agreed to update its Corporate Contingency Plan. On August 15, 1997, DFAS issued Interim Change 1-97 to the DFAS Corporate Contingency Plan, DFAS Regulation 3020.26-R. Interim Change 1-97 requires managers to prepare contingency plans addressing continuing operations alternatives for systems affected by the Y2K computer problem.

Contingency Planning Guidance. The DoD Y2K Management Plan addresses some of the requirements for an adequate contingency plan. The DFAS Corporate Contingency Plan, DFAS Regulation 3020.26-R, establishes the requirement for systems to establish continuity of operations plans.

DoD Y2K Management Plan, Version 1.0, April 1997. The DoD Y2K Management Plan states that contingency plans must be established when systems exit the assessment phase of the five-phased approach. The DoD Y2K

DoD Y2K Management Plan, Version 1.0, April 1997. The DoD Y2K Management Plan states that contingency plans must be established when systems exit the assessment phase of the five-phased approach. The DoD Y2K Management Plan states that realistic contingency plans should be established for each system, to include the development and activation of manual procedures or alternative contracted methods that ensure continuity of core processes. The Plan requires that contingency plans be updated as Y2K conversion progresses. The pending updated version of the DoD Y2K Management Plan is expected to include more detailed requirements for contingency plans. In addition, the updated version of the Plan expands the dates that may cause systems failure. Although December 31, 1999, represents one of the more critical dates that will determine the Y2K operability of a system, computer systems may experience Y2K related failures far ahead of that time. Dates that have been identified as potential failure dates include January 1, 1999, and October 1, 1999.

DFAS Corporate Contingency Plan, DFAS Regulation 3020.26-R, May 1997. The DFAS Corporate Contingency Plan documents management's responsibility to develop a contingency plan. Managers must conduct risk assessments for all critical systems impacted by the Y2K problem and for noncritical systems that provide data to critical systems. Managers are required to prepare contingency plans addressing alternatives for continuing operations in the event Y2K renovations are not completed on time, or if the renovated and replacement systems fail to operate properly.

DFAS Y2K Management Plan, Version 1.0, December 1997. The DFAS Y2K Management Plan documents strategic guidance for all DFAS information technology, software, and systems facing a Y2K problem. This plan focuses on Y2K resolution efforts throughout DFAS to ensure that no system failures occur because of Y2K problems. The DFAS Y2K Management Plan requires the development of a contingency plan for all systems critical to the DFAS mission and systems that feed a critical system. A contingency plan is required regardless of whether the system is categorized as compliant, being developed as compliant, being changed, or being replaced.

OMB Progress on Y2K Conversion Report, February 15, 1998. The OMB tasked the CIO Council to develop Government-wide best practices for contingency planning. The Council is working with GAO, which has developed a business continuity and contingency planning guide. Subsequently, the OMB adopted the GAO planning guide, " Y2K Computing Crisis: Business Continuity and Contingency Planning," for Federal agency use.

GAO "Y2K Computing Crisis: Business Continuity and Contingency Planning" (GAO/AIMD-10.1.19), August 1998. To aid Federal agencies in reducing the risk of Y2K-related business failures, GAO has developed a business continuity and contingency planning guide. The guide describes many of the necessary elements for an adequate contingency plan. According to the guide, each contingency plan should provide a risk assessment and processing alternatives and procedures, and should identify resources, activation triggers, staff roles, and identify methods of testing.

Elements of Contingency Plans

A contingency plan should address the actions to be taken during a problem and after a problem results in degraded system performance.

Risk Assessment. A risk assessment should be performed by business managers to identify how a system or device might fail and the potential impact of each failure. A risk assessment is essential in determining the effect of system failure on an agency's core business processes. It can be used to estimate damage, loss, or harm that may result from system failure. The following factors may be considered when assessing risk:

- the status of Y2K renovation and testing of systems,
- the total number of dependent systems and processes,
- the effect of failure on business operations, and
- the number of customers who would be affected.

Without a risk assessment, the contingency plan may not address all possible Y2K failure scenarios. The risk assessment helps management become aware of all system vulnerabilities and the effect on core business processes.

Processing Alternatives. In the event of system failure, system managers should select a strategy that is practical, cost-effective, and provides a high level of confidence in recovery capability. Strategies may implement manual, automated, or contract procedures and should be communicated to the appropriate staff and affected customers. Other factors that may be considered when selecting an alternative process are:

- the minimum acceptable level of output for core business processes,
- the time needed to acquire, test, and implement the alternative, and
- the cost to acquire, test, or train personnel on the alternative strategy.

Without assessing possible alternatives, management may not have adequate resources available to implement a contingency plan in the event of a Y2K failure.

Trigger Procedures. A trigger defines the condition or event that activates the contingency plan. The deployment schedule for the contingency plan and the implementation schedule for the system being replaced or renovated are elements that may be used to define the trigger. Without defining a trigger mechanism, management may lengthen the amount of time elapsed before the contingency plan is activated.

Staff Roles. A team should be established to pinpoint problems and provide the expertise to correct the problems. This team would be responsible for managing the implementation of contingency plans and operational problems, including potential failures of systems and their data exchanges. Contact telephone numbers of all personnel involved should be confirmed and updated regularly. Establishing staff roles helps management become aware of specific personnel responsible for activating and implementing the contingency plan.

Testing. Contingency plans should be tested to ensure that alternative methods are realistic and executable. Testing validates that all processes meet specifications in the event of an emergency and helps team members understand their roles and responsibilities. The testing process may also identify deficiencies, possible shortcomings, or procedural problems. Contingency plan testing establishes whether alternative business process meet an acceptable level of performance and whether the plan can be implemented within a specified period of time.

Review of DFAS Contingency Plans

Existence of DFAS Contingency Plans. We selected 30 mission-critical, migratory, and payment systems. (See Appendix A for the audit scope and methodology and Appendix C for a list of systems selected for review.) We met with system managers for 29 of the selected systems. Of the 29 systems reviewed, 21 had established contingency plans. We reviewed the contingency plans and discussed the adequacy of those plans with the system managers. During our review, we found that DFAS system-level contingency plans varied greatly in depth and scope. Though many DFAS system managers were able to provide written documentation of a contingency plan, nearly all plans lacked basic information needed to implement and manage a Y2K-related contingency.

Adequacy of DFAS Guidance for Contingency Plans. The DFAS Y2K Management Plan requires that a contingency plan be developed prior to exiting the renovation phase. The DFAS Director, Information and Technology, stated that the requirements conflicted because DFAS focused all functional and technical efforts on identifying, assessing, and changing systems affected by Y2K, rather than on contingency planning. This decision was based on the criticality of renovating the numerous financial systems that make payments.

We recognize that the expectation of having a comprehensive, fully developed contingency plan prior to exiting the assessment phase for every system was somewhat impractical. However, all of the 19 systems we reviewed that must progress through the 5 phases are beyond the assessment phase and still need contingency plans with much higher levels of detail than reflected during our review.

Examples of DFAS Contingency Plans. On a monthly basis, DFAS processes more than 9.8 million payments to DoD personnel and more than 1 million payments to DoD vendors and contractors, with a monthly disbursing total exceeding $22 billion. Several contingency plans for systems that process a large number of these payments stated that manual procedures would be implemented in the event of system failure. Many contingency plans were a single page and contained only a statement that processes would be performed manually. Further, these plans did not include the necessary elements of a contingency plan, such as a risk assessment, processing alternatives, trigger procedures, staff roles, and contingency plan testing. In addition, these contingency plans did not have adequate evaluations of the magnitude and complexity of the systems, or a detailed description of manual procedures. Examples of systems that had not yet developed adequate contingency plans include:

- Integrated Accounts Payable System (IAPS), which processes more than 1.8 million invoices for DoD vendors and contractors, exceeding $17 billion annually.

- Integrated Payments and Collections System (IPC), which processes approximately 6.2 million vouchers annually for payments to military and civilian personnel and DoD vendors, as well as travel payments.

- Defense Transport Payment System, which processes 3.2 million transportation billing documents and pays approximately $1.7 billion annually for the Army, Air Force, and other DoD activities.

- Defense Joint Military Pay System, which processes 2.1 million pay accounts with a monthly payroll of $2.6 billion.

Other systems without adequate contingency plans include the Integrated Automated Travel System, the Commercial Accounts Payable System, the Standard Finance System (SRD-1), and the Defense Civilian Pay System (DCPS).

The DCPS system maintains pay, leave entitlement, and other pertinent employee data for about 740,000 civilian employees. The DCPS project managers acknowledged shortcomings in the DCPS Y2K contingency plan and requested that the IG, DoD, provide feedback. We met with DCPS project managers to discuss some of the necessary elements for contingency plans and suggested areas of improvement based on the GAO planning guide, "Y2K Computing Crisis: Business Continuity and Contingency Planning" (GAO/AIMD-10.1.19), August 1998. The DCPS project managers were receptive to our comments and suggestions for the DCPS contingency plan. The DCPS project managers have actively worked with us to establish the necessary elements in the DCPS contingency plan.

Contingency Plans for Jointly Owned Systems. We reviewed three systems, the Mechanization of Contract Administration Services (MOCAS) system, the Base Operations Support System, and the Standard Automated Materiel Management System, that DFAS relies on to perform critical operations, but does not fully control. Should those systems fail, DFAS must ensure that adequate and detailed contingency plans are in place for DFAS business operations. For example, DFAS uses the MOCAS system to pay more than 1.2 million contractor invoices valued at more than $69 billion annually. MOCAS is jointly owned by DFAS and the Defense Logistics Agency (DLA); DFAS only owns 35 percent of a system. For the MOCAS system, DFAS managers stated that they are relying on the contingency plan established by DLA. However, the MOCAS contingency plan established by DLA does not adequately address the DFAS business operations for making payments to the contractor if the MOCAS system fails.

DFAS must either coordinate with DLA to ensure that DFAS operations are addressed in a contingency plan or establish independent contingency plans.

Management Actions Taken

On April 1, 1998, we met with the DFAS Y2K project staff and the DFAS Plans and Management Headquarters to discuss the status of contingency plans. We collectively identified some elements of an adequate contingency plan. This meeting resulted in an agreement that more attention was required to ensure that adequate contingency plans are established.

On April 20, 1998, we sent a memorandum to the DFAS Director, Information and Technology, on issues concerning the DFAS Status of Contingency Plans (see Appendix D). The DFAS Director, Information and Technology, responded in a memorandum issued on June 1, 1998 (see Appendix F). The DFAS Director, Information and Technology, agreed with the issues identified, and discussed actions under way to correct deficiencies in the contingency plans for all DFAS critical systems and systems that feed critical systems.

In response to our concerns about contingency plans, DFAS issued the Y2K Contingency Planning Guidance on August 24, 1998. The guidance is an overall plan for establishing comprehensive contingency plans. Y2K contingency planning issues have been incorporated in this overall plan. The guidance addresses the necessary elements for contingency plans, as outlined in the GAO planning guide, "Y2K Computing Crisis: Business Continuity and Contingency Planning," August 1998. The DFAS Contingency Planning Guidance requires DFAS business managers, system managers, and directors at DFAS Centers and Operating Locations to review and approve system-level contingency plans. This is critical, since system users must understand their responsibilities during activation of a contingency plan. This guidance will help system managers evaluate existing contingency plans and determine areas that require additional detail.

Conclusion

DFAS is placing a high priority on Y2K contingency planning, although it is somewhat behind schedule and more needs to be done to ensure the completeness and practicality of the plans. System managers did not have adequate guidance on the elements required in a contingency plan to manage a Y2K-induced failure. Contingency plans must be fully developed and tested prior to any potential Y2K failure of those systems.

System managers expressed concern that detailed contingency plans were unnecessary because of the low likelihood of activation. This attitude needs to be discouraged. Although the probability of activating a contingency plan is uncertain, adequate contingency plans should be established for critical systems, and systems that feed critical systems, as soon as possible. We believe that DFAS should focus efforts on contingency planning to ensure that systems critical to the DFAS mission have adequate contingency plans in place. These contingency plans should; at a minimum, address the elements identified in the GAO planning guide, "Y2K Computing Crisis: Business Continuity and Contingency Planning." DFAS must also coordinate contingency plans with its customers, users, and interface partners.

We commend DFAS for responding to the issues identified in this report and for taking prompt action. The approach established by DFAS in the recently issued DFAS Contingency Planning Guidance should greatly improve the reliability and consistency of system-level contingency plans. Ensuring that system managers follow the guidance should further reduce the risk of Y2K-related system failure.

Recommendations, Management Comments, and Audit Response

We recommend that the Director, Information and Technology, Defense Finance and Accounting Service:

1. Establish a verification mechanism to ensure that system managers have developed contingency plans that meet the requirements of the DFAS Y2K Contingency Planning Guidance.

Management Comments: DFAS concurred, stating that the DFAS system manager, Center Director, and headquarters functional representative must sign and review Y2K Contingency Plans as outlined in the DFAS Y2K Contingency Planning Guidance. In addition, the DFAS Y2K project officer will track completion of the Y2K Contingency Plans.

2. Ensure that Defense Finance and Accounting Service systems that are jointly owned have adequate contingency plans addressing Defense Finance and Accounting Service business processes.

Management Comments: DFAS concurred, stating that it is developing Core/Core Support Business Process contingency plans.

Audit Response: The corrective actions by DFAS met the intent of our recommendations. Therefore, management comments are considered responsive and no further comments are required.

Finding B. DFAS Cost Reporting for Y2K Initiatives

DFAS reported incomplete Y2K costs and underreported Y2K cost estimates in the OMB Quarterly Report. In February 1998, DFAS reported costs totaling $32 million to ASD($C^3$I) for inclusion in DoD's quarterly report to OMB. The inaccuracies occurred because DFAS did not include all of the necessary cost elements identified in the DoD Y2K Management Plan. As a result, DFAS did not have reliable cost estimates for its Y2K initiatives. In June 1998, DFAS increased its Y2K cost estimate to about $40 million. Unreliable cost estimates could cause DFAS to improperly prioritize funding for system changes, and DFAS may not be able to effectively redirect resources from other activities.

Review of Cost Estimates

We reviewed documentation supporting Y2K cost estimates for the DFAS systems reported quarterly to OMB by ASD(C^3I). We met with systems managers to determine how cost estimates were being developed. We compared cost estimates reported on the January 1998 Cost Requirements Report to documents supporting system-level Y2K cost estimates. We did not evaluate the methodology used to derive the individual costs that composed the total system-level Y2K estimates. We evaluated the inclusion of certain cost elements and factors within the total system-level Y2K estimates.

Y2K Cost Reporting Requirements

OMB Y2K Cost Guidance. OMB has established multiple guidelines for costing technology investments, including those that are Y2K-related.

- OMB Memorandum No. 97-02, "Funding Information Systems Investments," October 25, 1996, outlines the funding policy for all investments in major information systems, including the requirement that systems investments be consistent with an agency's Y2K compliance plan. To maintain awareness, OMB monitors agencies' progress in meeting Y2K compliance.

- OMB Report, "Getting Federal Computers Ready for 2000," February 6, 1997, states that Y2K cost estimates should include the costs of identifying Y2K problems, evaluating cost-effectiveness, and making system changes, as well as testing the systems and developing contingency plans in case of system failure. However, the estimate should not include the costs of upgrades or replacements that would otherwise occur as part of the normal system life cycle.

- OMB Circular No. A-11, section 43, "Data on Acquisition, Operation, and Use of Information Technology," describes some of the costs to be included for system estimates, including costs from the following categories: equipment hardware, software, support service, supplies, personnel compensation and benefits, and other costs.

DFAS Cost Guidance. DFAS has also established guidance for costing Y2K efforts. The DFAS Y2K Management Plan states that system managers must include a cost estimate, called the Cost Requirements Report, within the DFAS monthly reports on the Y2K problem. This report tracks the estimated costs for Y2K. The estimate should cover the entire effort from Y2K analysis through implementation, including functional and technical tasks. Further, the DFAS Y2K Management Plan states that the estimate should encompass only Y2K changes, not other system changes being made at the same time.

According to the DoD Y2K Management Plan, system costs include a number of factors that affect the Y2K compliance of a system. The cost estimates for Y2K should include the costs for modifying software, building the test environment, buying tools and services, adding hardware, upgrading operating system software, purchasing commercial products, and any related items. DoD Components can use a combination of cost metrics developed by the Gartner Group, the MITRE Corporation, and internal Component estimates. The DoD Component may base cost estimates on in-house models or actual fixes, but the Component must identify the methodology used.

Reliability of DFAS Y2K Cost Estimates. DFAS Y2K system cost estimates as reported to OMB and ASD(C^3I) did not represent complete or reliable assessments of the costs actually required to make the systems Y2K compliant. As of February 1998, DFAS reported total costs of $32 million for Y2K OMB reporting purposes. The DoD Y2K Management Plan includes a Y2K cost factor checklist that identifies additional cost factors that may be incurred. The following are some cost factors in the DoD Y2K Management Plan that should be included in a system's Y2K cost estimates, if applicable:

- Application software,
- Databases and files,
- Y2K tool support,
- Hardware and system software,
- External interfaces and middleware,
- System plans,
- Miscellaneous system-related information,
- Y2K management, and
- Y2K testing.

During the audit, we obtained cost documentation and system change requests for selected systems and met with system managers to determine what costs are being reported. We also obtained the DFAS Cost Requirements Report for January 1998, which details the DFAS reporting of system costs for Y2K changes. With particular attention to functional costs, which are costs for items such as acceptance testing and contingency planning, we compared the cost documentation with the Cost Requirements Report for January 1998, and determined that the costs were incomplete and underreported.

Several of the system cost estimates reviewed, included only the system change request (a form used by DFAS to initiate a change to a system) cost estimate. The system change request cost estimate usually included the technical (i.e., programming and unit testing) costs and usually did not include the functional (i.e., acceptance testing, contingency plan preparation, implementation costs) costs. The systems that underreported costs by not including functional costs are:

- Defense Retiree Annuitant Pay System-Annuitant Pay Subsystem (DRAS-APS). The DRAS-APS processes about 254,000 annuity accounts with a monthly payroll exceeding $139 million for annuitants. In the Cost Requirements Report for January 1998, DFAS reported a total cost of $686,000 for DRAS-APS.

- IAPS, which processes more than 1.8 million invoices for DoD vendors and contractors, exceeding $17 billion annually. In the Cost Requirements Report for January 1998, DFAS reported a total cost of $1,044,000 for IAPS.

Need for Reliable Cost Estimates

DFAS system managers need to establish complete and accurate cost estimates for making DFAS systems Y2K compliant as soon as possible. The cost estimates should be updated throughout the five phases, and these updates should be reported to OMB and ASD(C^3I) so that complete and reliable cost estimates are available to determine the impact of the Y2K efforts. By underreporting Y2K system cost estimates, DFAS may not effectively allocate resources, track Y2K impact on systems or the progress of system changes, or resolve funding issues for Y2K efforts. Some functional costs for in-house system changes will be incurred regardless of Y2K efforts, but if these resources are relevant to Y2K, they should be considered as outlined in the DFAS Y2K Management Plan.

Management Actions Taken

On May 4, 1998, we sent a memorandum to the DFAS Director, Information and Technology, concerning the cost reporting of DFAS Y2K initiatives (see Appendix E). The Director, Information and Technology, responded to our memorandum on June 9, 1998 (see Appendix G). The Director, Information and Technology, agreed that initial cost estimates for DFAS systems were incomplete and did not include all necessary elements identified in the DoD Y2K Management Plan.

In February 1998, DFAS reported a total cost of $32 million for Y2K for OMB reporting purposes. DFAS has implemented corrective actions to address the incomplete cost estimates. In the June 9, 1998, memorandum, DFAS directed that all system managers reassess cost estimates to ensure that all elements are addressed. DFAS emphasized that system managers must verify that all functional costs (i.e., acceptance testing and contingency plan preparation) are included in their Y2K costs. DFAS also directed system managers to periodically review cost estimates as DFAS moves toward Y2K compliance for its systems. In the DFAS memorandum, the DFAS Director, Information and Technology, stated that the Y2K cost estimate had been increased to about $40 million. This amount includes costs for DFAS systems and DFAS systems that are jointly owned. The total cost estimate was increased because of the reevaluation of the original cost estimates and the inclusion of elements that had originally been omitted. The DFAS Director, Information and Technology, stated that DFAS will continue to fund Y2K costs from existing financial systems budgets, and if additional Y2K costs are identified, DFAS will reprioritize the work load and make the necessary funds available.

Conclusion

We commend DFAS for responding to the issues identified in this report and for taking prompt action. DFAS has directed system managers to reassess cost estimates and verify that cost elements are addressed. This will result in more accurate and reliable Y2K cost estimates. If additional Y2K costs are identified, DFAS will reprioritize the current work load and make the necessary funds available. The corrective actions should assist DFAS in developing complete and reliable cost estimates. Reliable cost estimates are important to accurately reflect the Y2K impact and to facilitate DFAS allocation of funds by redirecting resources from other activities. Because of the actions taken by DFAS, we make no recommendations in this finding.

Part II - Additional Information

Appendix A. Audit Process

This is one of a series of reports being issued by the IG, DoD, in an informal partnership with the CIO, DoD, to monitor DoD efforts to address the Y2K computing challenge. For a list of audit projects addressing this issue, see the Y2K web page on the IGnet at www.ignet.gov.

Scope

This report was based on audit field work performed from February through September 1998 at the DFAS Centers in Indianapolis, Indiana; Denver, Colorado; Columbus, Ohio; and Kansas City, Missouri; Headquarters, DFAS; and Financial Systems Activities. Systems were selected from the DFAS January 1998 monthly report submitted to the Director, Information and Technology. The January 1998 monthly report showed that DFAS was tracking 179 finance and accounting systems for Y2K purposes. We selected 30 of the 179 systems for review (see Appendix C for a list of the systems selected for review). The 30 systems selected are primarily classified as migratory, payment, and mission-critical systems. Three of these systems are jointly owned by DFAS and DLA. With DFAS ownership less than 50 percent, Y2K compliance of these systems is mostly the responsibility of the majority owner, DLA.

We reviewed 29 of the 30 systems located at the DFAS Indianapolis, Denver, Columbus, and Kansas City Centers and at Headquarters, DFAS. One of the 30 systems, the Defense Joint Accounting System, was removed from our sample because the system was not scheduled to be fully implemented before January 1, 2000. We evaluated the reliability of the DFAS monthly reports and the accuracy and completeness of information in the quarterly report submitted to the ASD(C^3I).

DoD-Wide Corporate-Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, the Department of Defense has established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objective and goal.

> **Objective:** Fundamentally reengineer the Department and achieve a 21st century infrastructure. **Goal:** Reduce costs while maintaining required military capabilities across all DoD mission areas. **(DoD-6)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objective and goal.

> **Financial Management Functional Area. Objective:** Reengineer DoD business practices. **Goal:** Modify existing systems and monitor new systems to be Year 2000 compliant. **(FM-4.3)**

General Accounting Office High-Risk Area. In its identification of risk areas, the General Accounting Office has specifically designated risk in resolution of the Y2K problem as high. This report provides coverage of this problem and of the overall Information Management and Technology high-risk area.

Methodology

We communicated with personnel in the Office of the ASD(C^3I) who issue guidance on Y2K reporting, collect Y2K information from the DoD Components, and submit the information to OMB. We also interviewed DFAS personnel who are responsible for Y2K monthly reports. We interviewed the DFAS Y2K project officer; the Y2K point of contact (POC) at the DFAS Indianapolis, Denver, Columbus, and Kansas City Centers; the Y2K POC at Headquarters, DFAS; and system managers in functional and technical areas.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Use of Technical Assistance. We met with technical experts in our Analysis, Planning, and Technical Support Directorate to discuss issues relating to ongoing evaluation efforts of the OS/390 operating system, interface agreements, testing plans, and software development and maintenance issues.

Audit Type, Dates, and Standards. We performed this financial-related audit from February through September 1998 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the IG, DoD.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Management Control Program. We did not review the management control program as it relates to the overall audit objective. DFAS and DoD identified Y2K as an uncorrected material weakness in their Annual Statements of Assurance for FYs 1996 and 1997.

Appendix B. Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed on the Internet at www.gao.gov. Inspector General, DoD, reports can be accessed on the Internet at www.dodig.osd.mil.

Appendix C. DFAS Systems Reviewed

No.	Acronym	System Name[1]	System Location	Y2K Phase[2]	Status[3]
1	DCPS	Defense Civilian Pay System	DFAS-HQ[4]	Renovation	Migratory
2	DDMS	Defense Debt Management System	DFAS-DE[5]	Renovation	Migratory
3	DJMS	Defense Joint Military Pay System	DFAS-HQ	Renovation	Critical
4	MCTFS	Marine Corps Total Force System	DFAS-HQ	Validation	Migratory
5	DRAS-APS	Defense Retiree & Annuitant Pay System - Annuitant Pay Subsystem	DFAS-DE	Renovation	Migratory
6	DTRS	Defense Transportation Pay System	DFAS-IN[6]	Compliant	Migratory
7	DPPS	Defense Procurement Payment System	DFAS-HQ	Being Developed Compliant	Migratory
8	SRD-1	Standard Finance System Redesign (Subsystem 1)	DFAS-IN	Renovation	Interim Migratory
9	IPC	Integrated Paying & Collecting System	DFAS-DE	Renovation	Interim Migratory
10	SIFS	Standard Industrial Fund System	DFAS-IN	Renovation	Migratory
11	SMAS	Standard Materiel Accounting System	DFAS-DE	Renovation	Migratory
12	STARFIARS-MOD	Standard Army Financial Inventory Accounting and Report Modernization	DFAS-IN	Compliant	Migratory
13	DBMS	Defense Business Management System	DFAS-CO[7]	Renovation	Migratory
14	SABRS	Standard Accounting Budgeting & Reporting System	DFAS-KC[8]	Compliant	Migratory
15	PBAS-FD	Program & Budget Accounting System – Funds Distribution	DFAS-IN	Renovation	Migratory
16	CPRRS	Civilian Personnel Resource Reporting System	DFAS-KC	Compliant	Critical
17	NAFCPS	Non Appropriated Funds Civilian Payroll System	DFAS-IN	Compliant	Critical
18	FIABS	Financial Inventory Accounting & Billing System	DFAS-DE	Renovation	Migratory
19	DCMS	Departmental Cash Management System	DFAS-DE	Being Developed Compliant	Critical
20	EAS	Entitlement Automation System	DFAS-CO	Compliant	Critical
21	MOCAS	Mechanization of Contract Administration Services	DFAS-CO	Renovation	Critical
22	SAMMS	Standard Automated Material Management System	DFAS-CO	Renovation	Migratory
23	BOSS	Base Operations Support System	DFAS-CO	Renovation	Migratory
24	CAPS	Computerized Accounts Payable System	DFAS-IN	Renovation	Critical
25	IATS	Integrated Automated Travel System	DFAS-IN	Compliant	Critical
26	IAPS	Integrated Accounts Payable System	DFAS-DE	Validation	Critical
27	DOPS	Disbursing Office Processing System	DFAS-IN	Renovation	Critical
28	AFES	Automated Financial Entitlements System	DFAS-IN	To Be Replaced	Critical
29	DCAS	Defense Cash Accountability System	DFAS-HQ	Being Developed Compliant	Noncritical

Appendix C. DFAS Systems Reviewed

[1] Information based on DFAS January 1998 Monthly Report.

[2] An existing system can be certified as compliant through the five-phase process. The five-phase process is described in the background of this report. A system can be developed as Y2K compliant and confirmed through certification. A system may be replaced or retired by a migratory system.

[3] "Critical" refers to a financial system that provides information materially important to the agency's financial reporting or is necessary for the agency to effectively and efficiently fulfill its primary mission. "Migratory" refers an existing automated information system that is officially designated as a single AIS to support standard processes for a function.

[4] DFAS-HQ: Headquarters, DFAS.

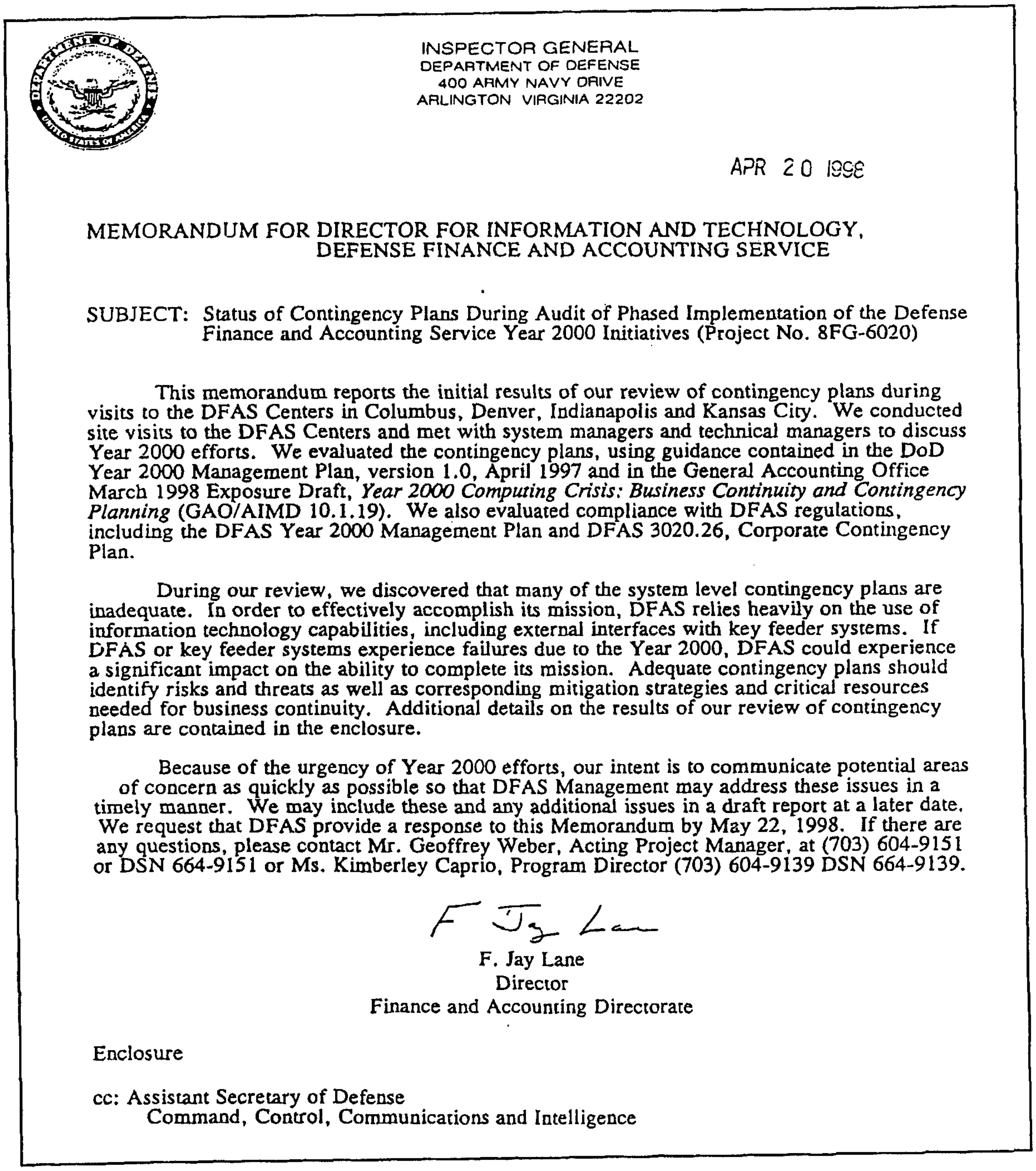
[5] DFAS-DE: DFAS Denver Center.

[6] DFAS-IN: DFAS Indianapolis Center.

[7] DFAS-CO: DFAS Columbus Center.

[8] DFAS-KC: DFAS Kansas Center.

Appendix D. IG, DoD, Memorandum to DFAS on Y2K Contingency Plans



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON VIRGINIA 22202

APR 20 1998

MEMORANDUM FOR DIRECTOR FOR INFORMATION AND TECHNOLOGY,
DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Status of Contingency Plans During Audit of Phased Implementation of the Defense Finance and Accounting Service Year 2000 Initiatives (Project No. 8FG-6020)

This memorandum reports the initial results of our review of contingency plans during visits to the DFAS Centers in Columbus, Denver, Indianapolis and Kansas City. We conducted site visits to the DFAS Centers and met with system managers and technical managers to discuss Year 2000 efforts. We evaluated the contingency plans, using guidance contained in the DoD Year 2000 Management Plan, version 1.0, April 1997 and in the General Accounting Office March 1998 Exposure Draft, *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD 10.1.19). We also evaluated compliance with DFAS regulations, including the DFAS Year 2000 Management Plan and DFAS 3020.26, Corporate Contingency Plan.

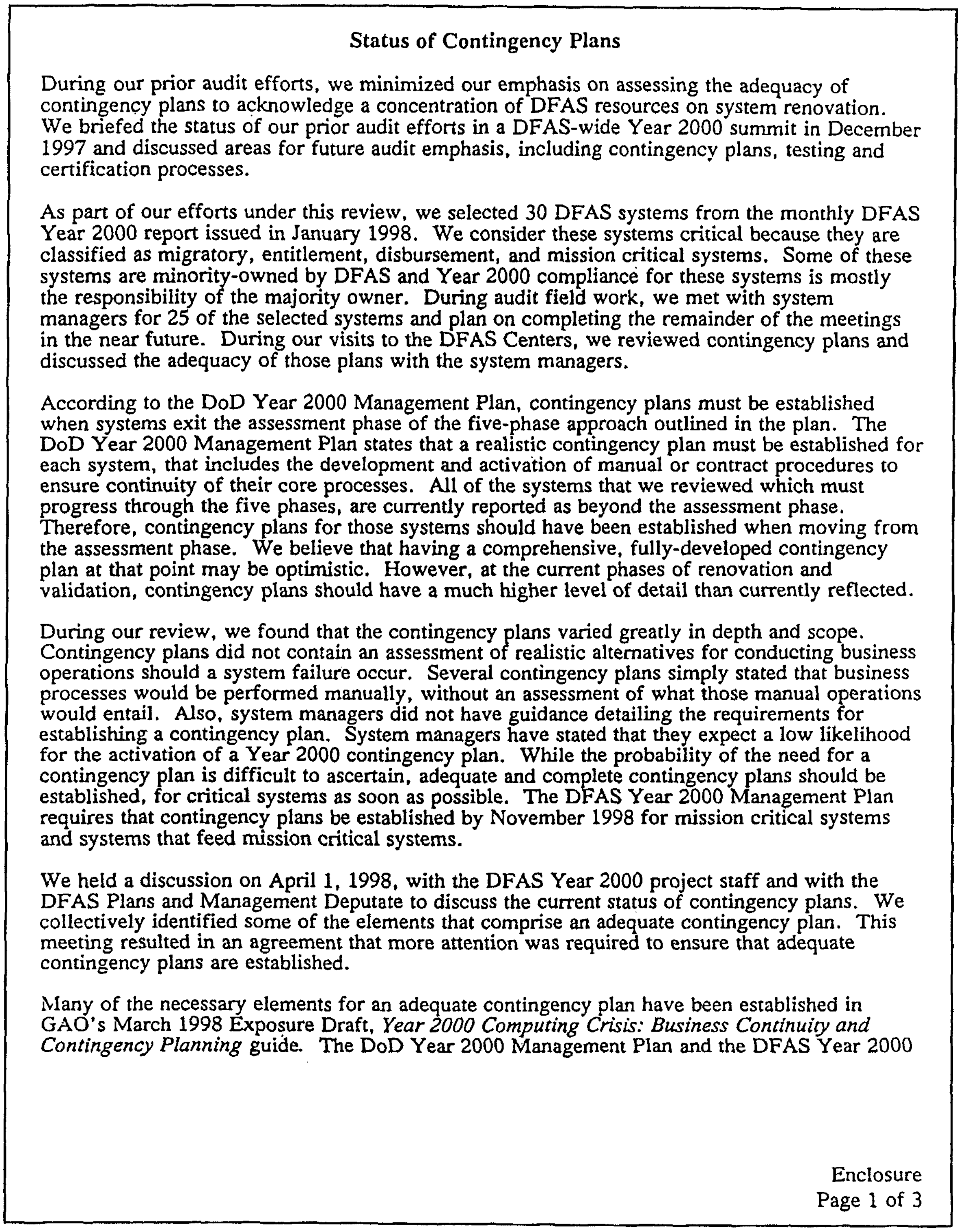
During our review, we discovered that many of the system level contingency plans are inadequate. In order to effectively accomplish its mission, DFAS relies heavily on the use of information technology capabilities, including external interfaces with key feeder systems. If DFAS or key feeder systems experience failures due to the Year 2000, DFAS could experience a significant impact on the ability to complete its mission. Adequate contingency plans should identify risks and threats as well as corresponding mitigation strategies and critical resources needed for business continuity. Additional details on the results of our review of contingency plans are contained in the enclosure.

Because of the urgency of Year 2000 efforts, our intent is to communicate potential areas of concern as quickly as possible so that DFAS Management may address these issues in a timely manner. We may include these and any additional issues in a draft report at a later date. We request that DFAS provide a response to this Memorandum by May 22, 1998. If there are any questions, please contact Mr. Geoffrey Weber, Acting Project Manager, at (703) 604-9151 or DSN 664-9151 or Ms. Kimberley Caprio, Program Director (703) 604-9139 DSN 664-9139.

F. Jay Lane
Director
Finance and Accounting Directorate

Enclosure

cc: Assistant Secretary of Defense
Command, Control, Communications and Intelligence



Status of Contingency Plans

During our prior audit efforts, we minimized our emphasis on assessing the adequacy of contingency plans to acknowledge a concentration of DFAS resources on system renovation. We briefed the status of our prior audit efforts in a DFAS-wide Year 2000 summit in December 1997 and discussed areas for future audit emphasis, including contingency plans, testing and certification processes.

As part of our efforts under this review, we selected 30 DFAS systems from the monthly DFAS Year 2000 report issued in January 1998. We consider these systems critical because they are classified as migratory, entitlement, disbursement, and mission critical systems. Some of these systems are minority-owned by DFAS and Year 2000 compliance for these systems is mostly the responsibility of the majority owner. During audit field work, we met with system managers for 25 of the selected systems and plan on completing the remainder of the meetings in the near future. During our visits to the DFAS Centers, we reviewed contingency plans and discussed the adequacy of those plans with the system managers.

According to the DoD Year 2000 Management Plan, contingency plans must be established when systems exit the assessment phase of the five-phase approach outlined in the plan. The DoD Year 2000 Management Plan states that a realistic contingency plan must be established for each system, that includes the development and activation of manual or contract procedures to ensure continuity of their core processes. All of the systems that we reviewed which must progress through the five phases, are currently reported as beyond the assessment phase. Therefore, contingency plans for those systems should have been established when moving from the assessment phase. We believe that having a comprehensive, fully-developed contingency plan at that point may be optimistic. However, at the current phases of renovation and validation, contingency plans should have a much higher level of detail than currently reflected.

During our review, we found that the contingency plans varied greatly in depth and scope. Contingency plans did not contain an assessment of realistic alternatives for conducting business operations should a system failure occur. Several contingency plans simply stated that business processes would be performed manually, without an assessment of what those manual operations would entail. Also, system managers did not have guidance detailing the requirements for establishing a contingency plan. System managers have stated that they expect a low likelihood for the activation of a Year 2000 contingency plan. While the probability of the need for a contingency plan is difficult to ascertain, adequate and complete contingency plans should be established, for critical systems as soon as possible. The DFAS Year 2000 Management Plan requires that contingency plans be established by November 1998 for mission critical systems and systems that feed mission critical systems.

We held a discussion on April 1, 1998, with the DFAS Year 2000 project staff and with the DFAS Plans and Management Deputate to discuss the current status of contingency plans. We collectively identified some of the elements that comprise an adequate contingency plan. This meeting resulted in an agreement that more attention was required to ensure that adequate contingency plans are established.

Many of the necessary elements for an adequate contingency plan have been established in GAO's March 1998 Exposure Draft, *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* guide. The DoD Year 2000 Management Plan and the DFAS Year 2000

Management Plan also detail some of the elements that should be included in an adequate contingency plan and some of the scenarios that a contingency plan should address. Some of these elements include:

- a risk assessment,
- staff roles,
- processing alternatives,
- backup procedures, and
- manual or contract procedures.

The impending updated version of the DoD Year 2000 Management Plan is anticipated to include more detailed requirements for contingency plans.

If critical systems were to fail due to Year 2000 problems, DFAS could suffer a major impact on its ability to disburse payments to civilian and military personnel, contractors, vendors, retirees and annuitants. On a monthly basis, DFAS processes more than 9.8 million payments to DoD personnel and more than 1 million payments to DoD vendors and contractors with a monthly disbursing total exceeding $22 billion. The lack of adequate contingency plans for systems that are integral to those payment functions will likely lengthen the amount of time that will elapse before these payments can resume.

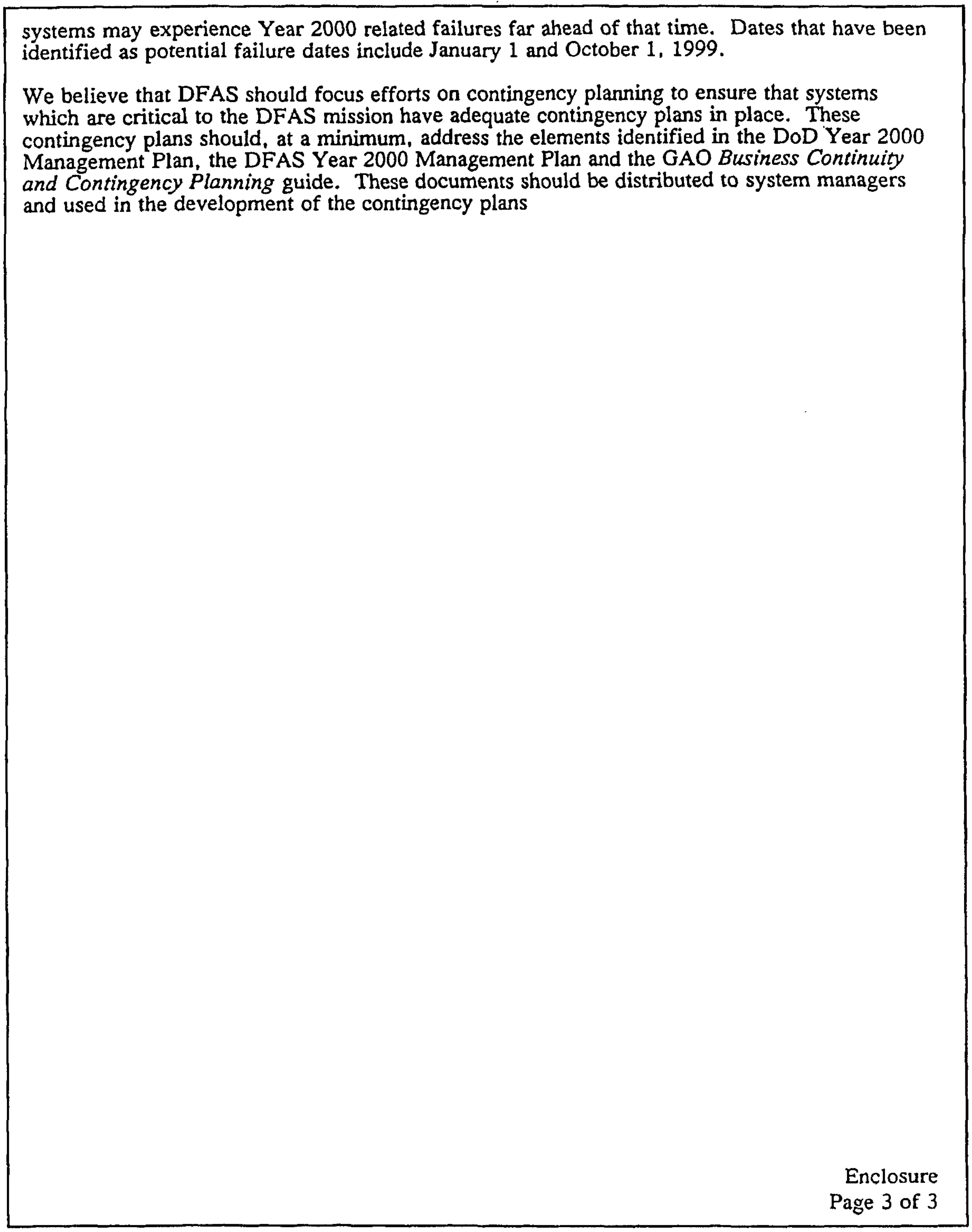
Several contingency plans for systems that process a large number of payments stated that manual procedures would be implemented in the event of system failure. Many of the contingency plans were no more than a single page in length and contained only a statement that processes would be performed manually. These plans did not address other elements of the contingency strategy and did not contain an evaluation of the magnitude or detailed description of the manual procedures. Examples of systems that did not have adequate contingency plans developed include:

- the Integrated Accounts Payable System (IAPS) which processes more than 1.8 million invoices for DoD vendors and contractors, exceeding $17 billion on an annual basis, and
- the Integrated Payments and Collections System (IPC) which processes approximately 6.2 million vouchers annually for payments to military and civilian personnel and DoD vendors as well as travel payments

Other systems without adequate contingency plans include the Integrated Automated Travel System (IATS), Commercial Accounts Payable System (CAPS) and the Mechanization of Contract Administration Services system (MOCAS).

DFAS will also face a challenge for those minority-owned systems that it relies upon for critical operations. Should those systems fail, DFAS must ensure that a realistic and feasible contingency plan is in place to address the DFAS business process for the minority-owned system. For example, the MOCAS system, which DFAS uses to pay more than 1 million contractor invoices valued at more than $65 billion annually, is majority-owned by the Defense Logistics Agency (DLA). For the MOCAS system, DFAS is relying on the contingency plan established by DLA, which does not adequately address contingency planning for the DFAS functions. DFAS must either coordinate with the majority owner to ensure that DFAS functions are addressed in a contingency plan or establish independent contingency plans for those minority-owned systems that address the DFAS functions within those systems.

It is crucial that contingency plans be fully developed, tested and implemented prior to any potential Year 2000 failure of those systems. While the December 31, 1999 date represents one of the more critical dates that will determine the Year 2000 operability of a system, the DFAS

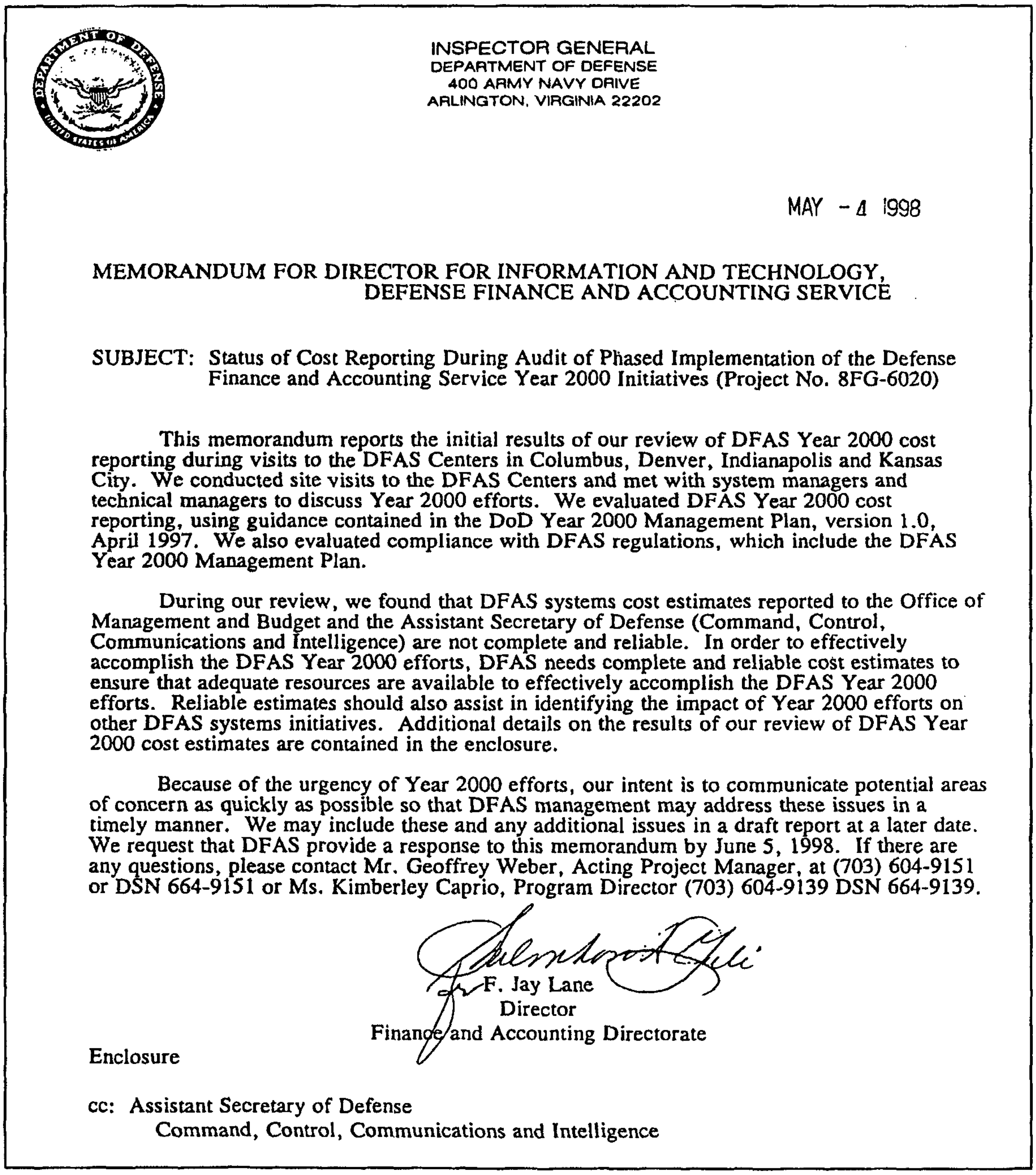


systems may experience Year 2000 related failures far ahead of that time. Dates that have been identified as potential failure dates include January 1 and October 1, 1999.

We believe that DFAS should focus efforts on contingency planning to ensure that systems which are critical to the DFAS mission have adequate contingency plans in place. These contingency plans should, at a minimum, address the elements identified in the DoD Year 2000 Management Plan, the DFAS Year 2000 Management Plan and the GAO *Business Continuity and Contingency Planning* guide. These documents should be distributed to system managers and used in the development of the contingency plans

Enclosure
Page 3 of 3

Appendix E. IG, DoD, Memorandum to DFAS on Y2K Cost Reporting



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202

MAY - 4 1998

MEMORANDUM FOR DIRECTOR FOR INFORMATION AND TECHNOLOGY,
DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Status of Cost Reporting During Audit of Phased Implementation of the Defense Finance and Accounting Service Year 2000 Initiatives (Project No. 8FG-6020)

This memorandum reports the initial results of our review of DFAS Year 2000 cost reporting during visits to the DFAS Centers in Columbus, Denver, Indianapolis and Kansas City. We conducted site visits to the DFAS Centers and met with system managers and technical managers to discuss Year 2000 efforts. We evaluated DFAS Year 2000 cost reporting, using guidance contained in the DoD Year 2000 Management Plan, version 1.0, April 1997. We also evaluated compliance with DFAS regulations, which include the DFAS Year 2000 Management Plan.

During our review, we found that DFAS systems cost estimates reported to the Office of Management and Budget and the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) are not complete and reliable. In order to effectively accomplish the DFAS Year 2000 efforts, DFAS needs complete and reliable cost estimates to ensure that adequate resources are available to effectively accomplish the DFAS Year 2000 efforts. Reliable estimates should also assist in identifying the impact of Year 2000 efforts on other DFAS systems initiatives. Additional details on the results of our review of DFAS Year 2000 cost estimates are contained in the enclosure.

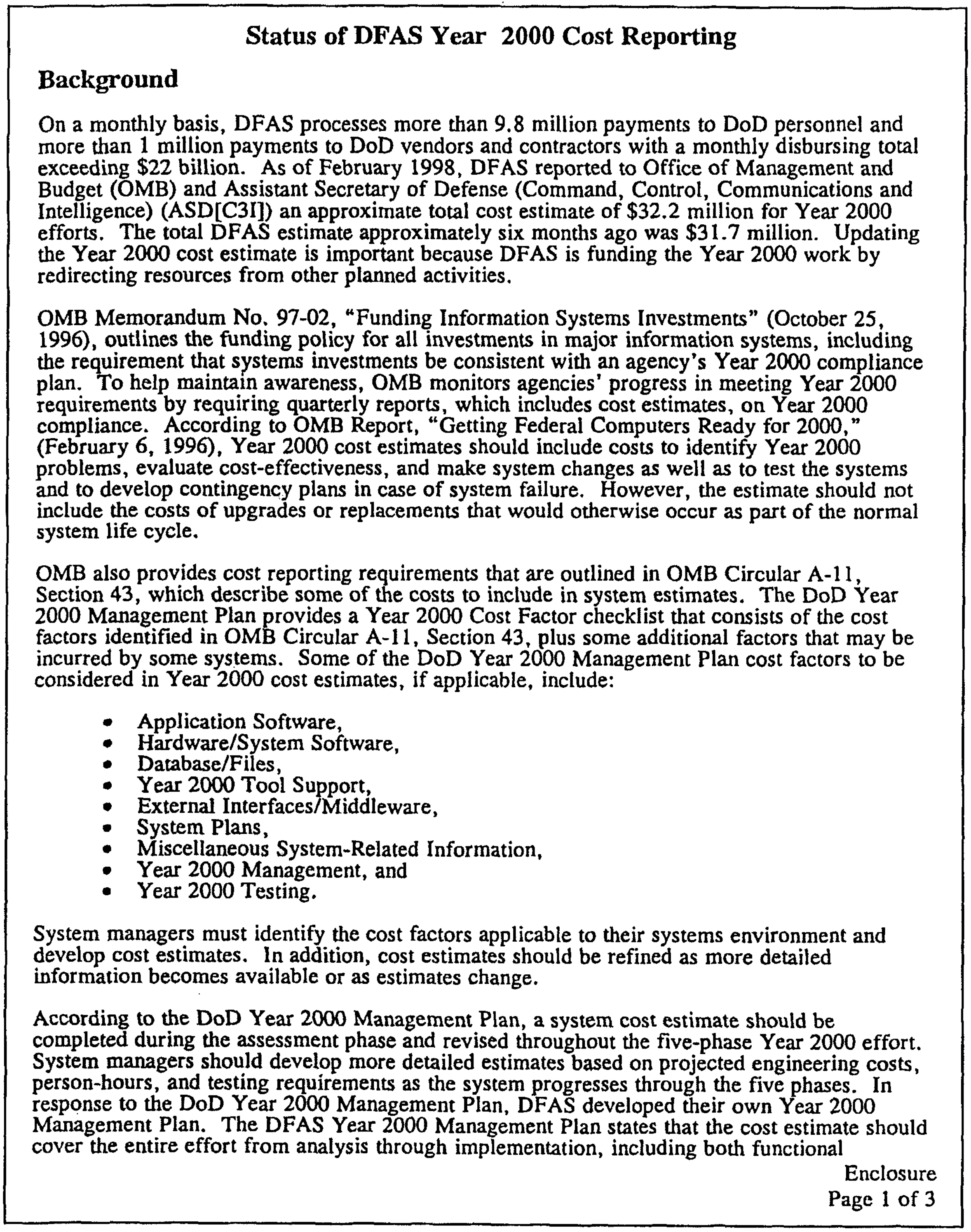
Because of the urgency of Year 2000 efforts, our intent is to communicate potential areas of concern as quickly as possible so that DFAS management may address these issues in a timely manner. We may include these and any additional issues in a draft report at a later date. We request that DFAS provide a response to this memorandum by June 5, 1998. If there are any questions, please contact Mr. Geoffrey Weber, Acting Project Manager, at (703) 604-9151 or DSN 664-9151 or Ms. Kimberley Caprio, Program Director (703) 604-9139 DSN 664-9139.

F. Jay Lane
Director
Finance and Accounting Directorate

Enclosure

cc: Assistant Secretary of Defense
Command, Control, Communications and Intelligence

Appendix E. IG, DoD, Memorandum to DFAS on Y2K Cost Reporting



Status of DFAS Year 2000 Cost Reporting

Background

On a monthly basis, DFAS processes more than 9.8 million payments to DoD personnel and more than 1 million payments to DoD vendors and contractors with a monthly disbursing total exceeding $22 billion. As of February 1998, DFAS reported to Office of Management and Budget (OMB) and Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD[C3I]) an approximate total cost estimate of $32.2 million for Year 2000 efforts. The total DFAS estimate approximately six months ago was $31.7 million. Updating the Year 2000 cost estimate is important because DFAS is funding the Year 2000 work by redirecting resources from other planned activities.

OMB Memorandum No. 97-02, "Funding Information Systems Investments" (October 25, 1996), outlines the funding policy for all investments in major information systems, including the requirement that systems investments be consistent with an agency's Year 2000 compliance plan. To help maintain awareness, OMB monitors agencies' progress in meeting Year 2000 requirements by requiring quarterly reports, which includes cost estimates, on Year 2000 compliance. According to OMB Report, "Getting Federal Computers Ready for 2000," (February 6, 1996), Year 2000 cost estimates should include costs to identify Year 2000 problems, evaluate cost-effectiveness, and make system changes as well as to test the systems and to develop contingency plans in case of system failure. However, the estimate should not include the costs of upgrades or replacements that would otherwise occur as part of the normal system life cycle.

OMB also provides cost reporting requirements that are outlined in OMB Circular A-11, Section 43, which describe some of the costs to include in system estimates. The DoD Year 2000 Management Plan provides a Year 2000 Cost Factor checklist that consists of the cost factors identified in OMB Circular A-11, Section 43, plus some additional factors that may be incurred by some systems. Some of the DoD Year 2000 Management Plan cost factors to be considered in Year 2000 cost estimates, if applicable, include:

- Application Software,
- Hardware/System Software,
- Database/Files,
- Year 2000 Tool Support,
- External Interfaces/Middleware,
- System Plans,
- Miscellaneous System-Related Information,
- Year 2000 Management, and
- Year 2000 Testing.

System managers must identify the cost factors applicable to their systems environment and develop cost estimates. In addition, cost estimates should be refined as more detailed information becomes available or as estimates change.

According to the DoD Year 2000 Management Plan, a system cost estimate should be completed during the assessment phase and revised throughout the five-phase Year 2000 effort. System managers should develop more detailed estimates based on projected engineering costs, person-hours, and testing requirements as the system progresses through the five phases. In response to the DoD Year 2000 Management Plan, DFAS developed their own Year 2000 Management Plan. The DFAS Year 2000 Management Plan states that the cost estimate should cover the entire effort from analysis through implementation, including both functional

Enclosure
Page 1 of 3

(i.e., system plans, acceptance testing, Year 2000 management, contingency plan preparation, implementation costs, Year 2000 tool support) and technical (i.e., programming for software, hardware and system software, and unit testing) tasks. The DFAS Year 2000 Management Plan further states that cost estimates should only encompass Year 2000 changes, not other changes being made at the same time.

Scope of Work Performed

As part of our efforts under this review, we selected 30 DFAS systems from the monthly DFAS Year 2000 report issued in January 1998. We consider these systems critical because they are classified as migratory, entitlement, disbursement, and mission critical systems. Three of the 30 systems are minority-owned by DFAS, and Year 2000 compliance for these systems is primarily the responsibility of the majority owner. We reviewed systems reported in the "to be changed" category which requires systems to progress through the five management plan phases identified as the awareness, awareness, renovation, validation, and implementation phases. We also reviewed systems reported in the "to be replaced," "compliant," and "being developed compliant" categories.

We met with system and technical managers for 27 of the selected systems and plan to meet with managers for the remaining five systems. Of the systems that we reviewed, those which must progress through the five phases are currently reported as beyond the assessment phase. We reviewed Year 2000 cost estimates for these systems that are reported quarterly to OMB by ASD(C3I). We did not evaluate the methodology used to calculate the individual costs to create the total system level Year 2000 estimates. We only evaluated the inclusion of certain costs within that total estimate.

Issue Identified

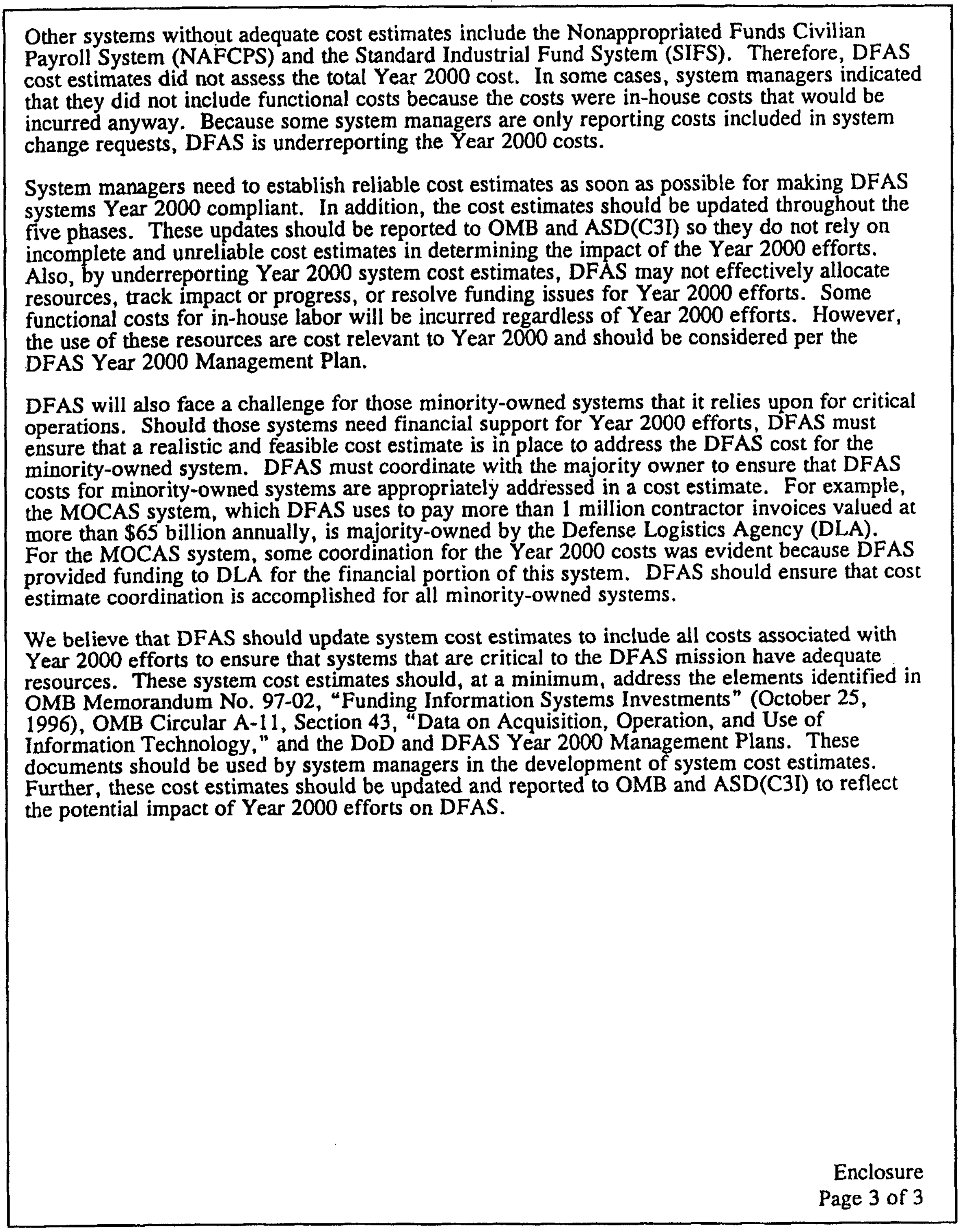
DFAS Year 2000 system cost estimates reported to OMB and ASD(C3I) do not contain a complete and reliable assessment of the costs actually required to make the systems Year 2000 compliant. Cost estimates did not contain all of the necessary elements identified in the DoD Year 2000 Management Plan Cost Factors checklist. The system cost estimates should, at a minimum, have addressed the elements identified in the DoD Year 2000 Management Plan. Several of the system cost estimates reviewed, included only the system change request (a form used by DFAS to initiate a change to a system) cost estimate. The system change request cost estimate usually included the technical (i.e., programming and unit testing) costs and usually did not include the functional (i.e., acceptance testing, contingency plan preparation, implementation costs) costs.

Some examples of systems that underreported their cost estimates by only including the costs of the system change requests are:

- The Defense Retiree and Annuitant Pay System (DRAS) which processes approximately 1.9 million retiree and 254 thousand annuity accounts with a monthly payroll exceeding $2.5 billion for retirees and $139 million for annuitants.

- The Integrated Accounts Payable System (IAPS) which processes more than 1.8 million invoices for DoD vendors and contractors, exceeding $17 billion on an annual basis.

- The Integrated Payments and Collections System (IPC) which processes approximately 6.2 million vouchers annually for payments to military and civilian personnel and DoD vendors as well as travel payments.



Other systems without adequate cost estimates include the Nonappropriated Funds Civilian Payroll System (NAFCPS) and the Standard Industrial Fund System (SIFS). Therefore, DFAS cost estimates did not assess the total Year 2000 cost. In some cases, system managers indicated that they did not include functional costs because the costs were in-house costs that would be incurred anyway. Because some system managers are only reporting costs included in system change requests, DFAS is underreporting the Year 2000 costs.

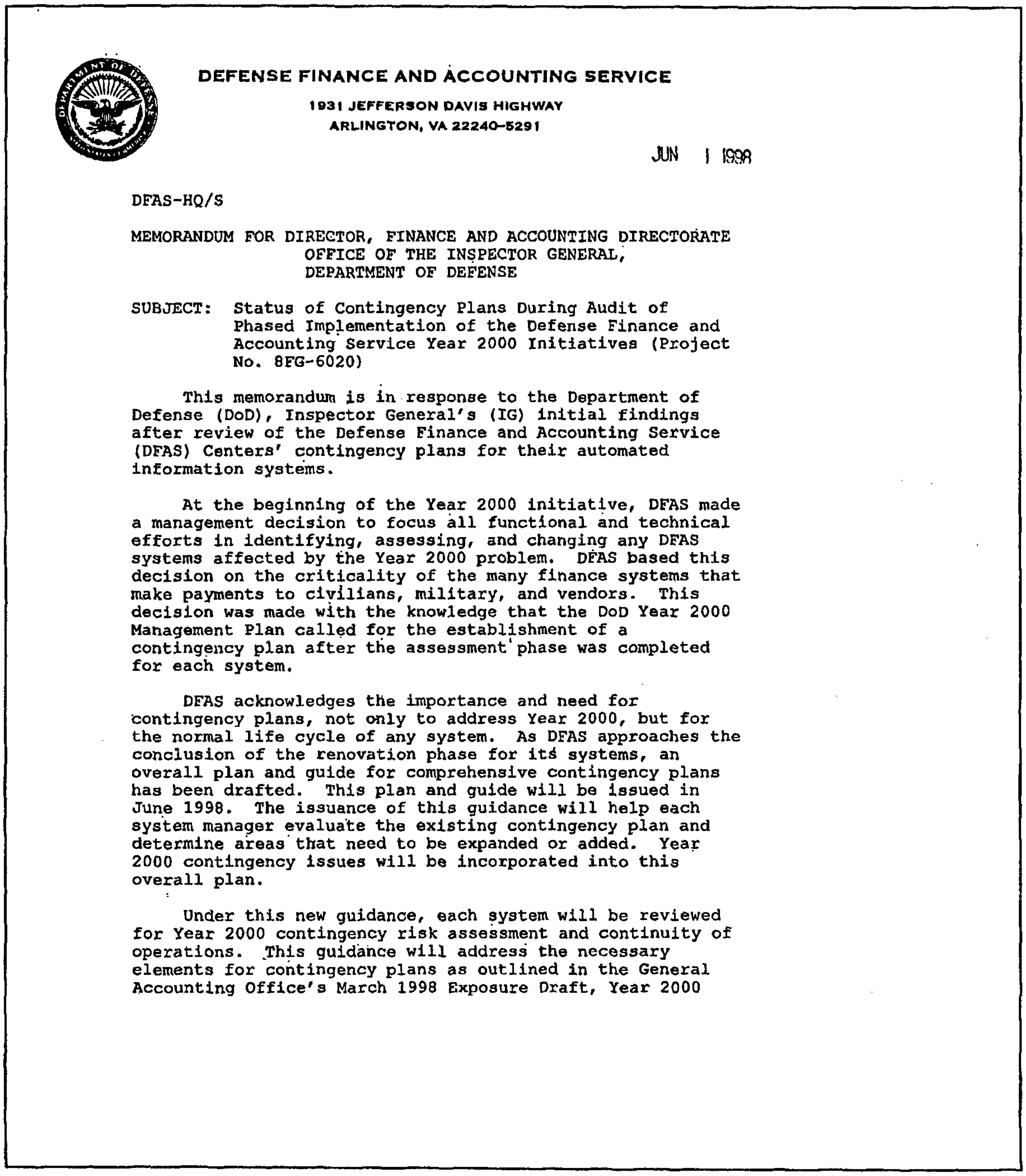
System managers need to establish reliable cost estimates as soon as possible for making DFAS systems Year 2000 compliant. In addition, the cost estimates should be updated throughout the five phases. These updates should be reported to OMB and ASD(C3I) so they do not rely on incomplete and unreliable cost estimates in determining the impact of the Year 2000 efforts. Also, by underreporting Year 2000 system cost estimates, DFAS may not effectively allocate resources, track impact or progress, or resolve funding issues for Year 2000 efforts. Some functional costs for in-house labor will be incurred regardless of Year 2000 efforts. However, the use of these resources are cost relevant to Year 2000 and should be considered per the DFAS Year 2000 Management Plan.

DFAS will also face a challenge for those minority-owned systems that it relies upon for critical operations. Should those systems need financial support for Year 2000 efforts, DFAS must ensure that a realistic and feasible cost estimate is in place to address the DFAS cost for the minority-owned system. DFAS must coordinate with the majority owner to ensure that DFAS costs for minority-owned systems are appropriately addressed in a cost estimate. For example, the MOCAS system, which DFAS uses to pay more than 1 million contractor invoices valued at more than $65 billion annually, is majority-owned by the Defense Logistics Agency (DLA). For the MOCAS system, some coordination for the Year 2000 costs was evident because DFAS provided funding to DLA for the financial portion of this system. DFAS should ensure that cost estimate coordination is accomplished for all minority-owned systems.

We believe that DFAS should update system cost estimates to include all costs associated with Year 2000 efforts to ensure that systems that are critical to the DFAS mission have adequate resources. These system cost estimates should, at a minimum, address the elements identified in OMB Memorandum No. 97-02, "Funding Information Systems Investments" (October 25, 1996), OMB Circular A-11, Section 43, "Data on Acquisition, Operation, and Use of Information Technology," and the DoD and DFAS Year 2000 Management Plans. These documents should be used by system managers in the development of system cost estimates. Further, these cost estimates should be updated and reported to OMB and ASD(C3I) to reflect the potential impact of Year 2000 efforts on DFAS.

Enclosure
Page 3 of 3

Appendix F. DFAS Memorandum on Y2K Contingency Plans



DEFENSE FINANCE AND ACCOUNTING SERVICE
1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

JUN 1 1998

DFAS-HQ/S

MEMORANDUM FOR DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE
OFFICE OF THE INSPECTOR GENERAL,
DEPARTMENT OF DEFENSE

SUBJECT: Status of Contingency Plans During Audit of Phased Implementation of the Defense Finance and Accounting Service Year 2000 Initiatives (Project No. 8FG-6020)

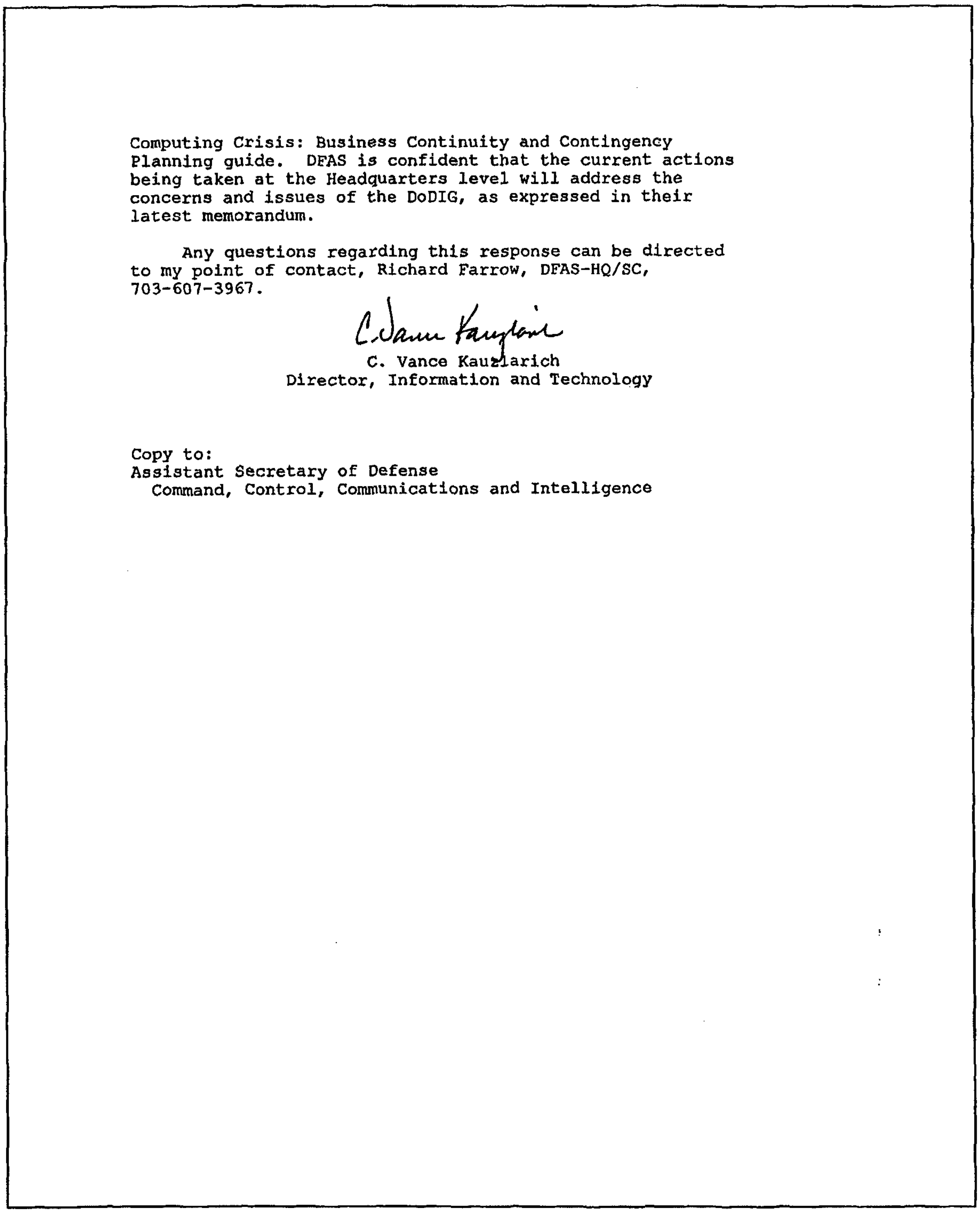
This memorandum is in response to the Department of Defense (DoD), Inspector General's (IG) initial findings after review of the Defense Finance and Accounting Service (DFAS) Centers' contingency plans for their automated information systems.

At the beginning of the Year 2000 initiative, DFAS made a management decision to focus all functional and technical efforts in identifying, assessing, and changing any DFAS systems affected by the Year 2000 problem. DFAS based this decision on the criticality of the many finance systems that make payments to civilians, military, and vendors. This decision was made with the knowledge that the DoD Year 2000 Management Plan called for the establishment of a contingency plan after the assessment phase was completed for each system.

DFAS acknowledges the importance and need for contingency plans, not only to address Year 2000, but for the normal life cycle of any system. As DFAS approaches the conclusion of the renovation phase for its systems, an overall plan and guide for comprehensive contingency plans has been drafted. This plan and guide will be issued in June 1998. The issuance of this guidance will help each system manager evaluate the existing contingency plan and determine areas that need to be expanded or added. Year 2000 contingency issues will be incorporated into this overall plan.

Under this new guidance, each system will be reviewed for Year 2000 contingency risk assessment and continuity of operations. This guidance will address the necessary elements for contingency plans as outlined in the General Accounting Office's March 1998 Exposure Draft, Year 2000

Appendix F. DFAS Memorandum on Y2K Contingency Plans



Computing Crisis: Business Continuity and Contingency Planning guide. DFAS is confident that the current actions being taken at the Headquarters level will address the concerns and issues of the DoDIG, as expressed in their latest memorandum.

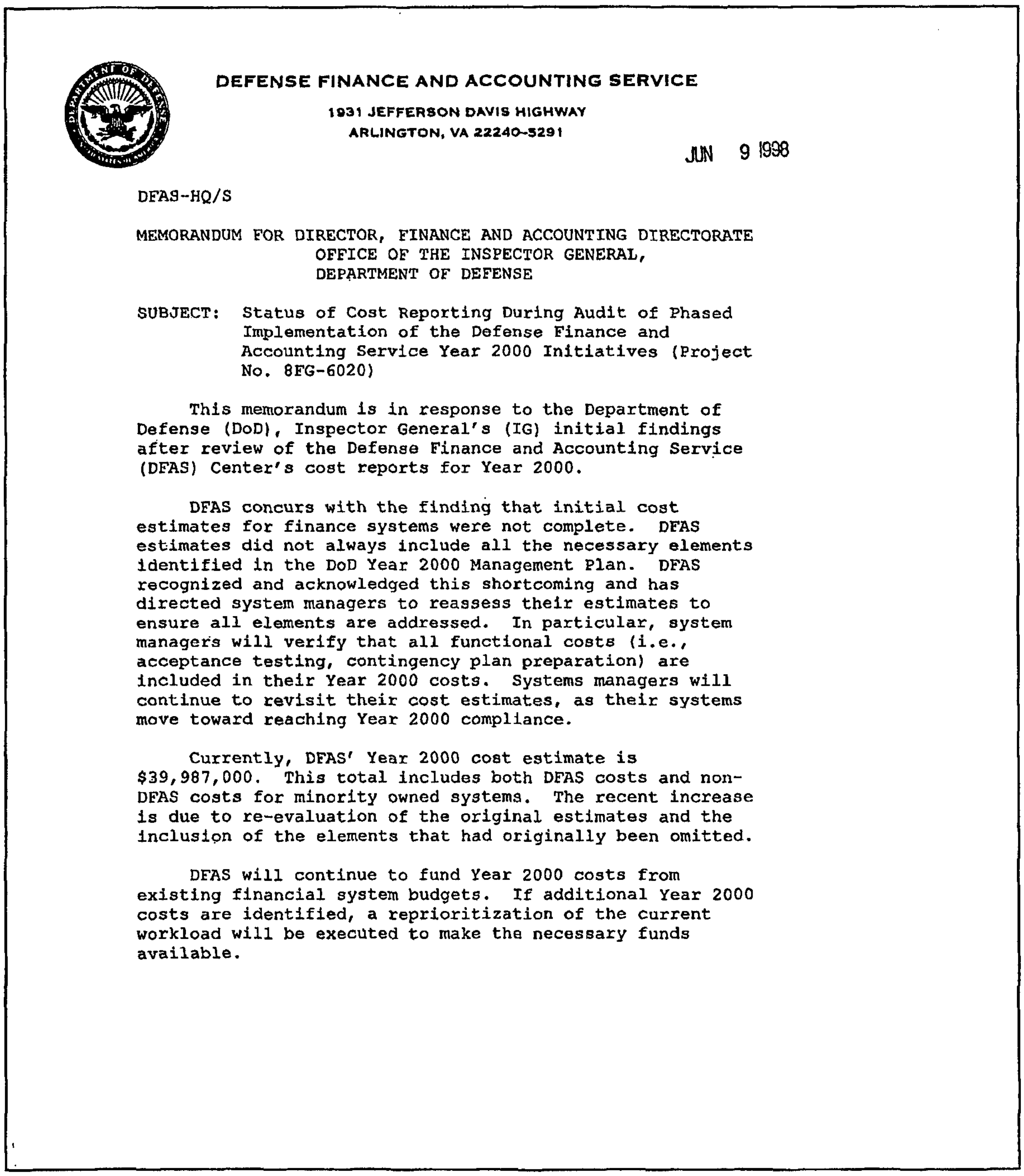
Any questions regarding this response can be directed to my point of contact, Richard Farrow, DFAS-HQ/SC, 703-607-3967.

C. Vance Kauzlarich

C. Vance Kauzlarich
Director, Information and Technology

Copy to:
Assistant Secretary of Defense
Command, Control, Communications and Intelligence

Appendix G. DFAS Memorandum on Y2K Cost Reporting



DEFENSE FINANCE AND ACCOUNTING SERVICE
1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

JUN 9 1998

DFAS-HQ/S

MEMORANDUM FOR DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE
OFFICE OF THE INSPECTOR GENERAL,
DEPARTMENT OF DEFENSE

SUBJECT: Status of Cost Reporting During Audit of Phased Implementation of the Defense Finance and Accounting Service Year 2000 Initiatives (Project No. 8FG-6020)

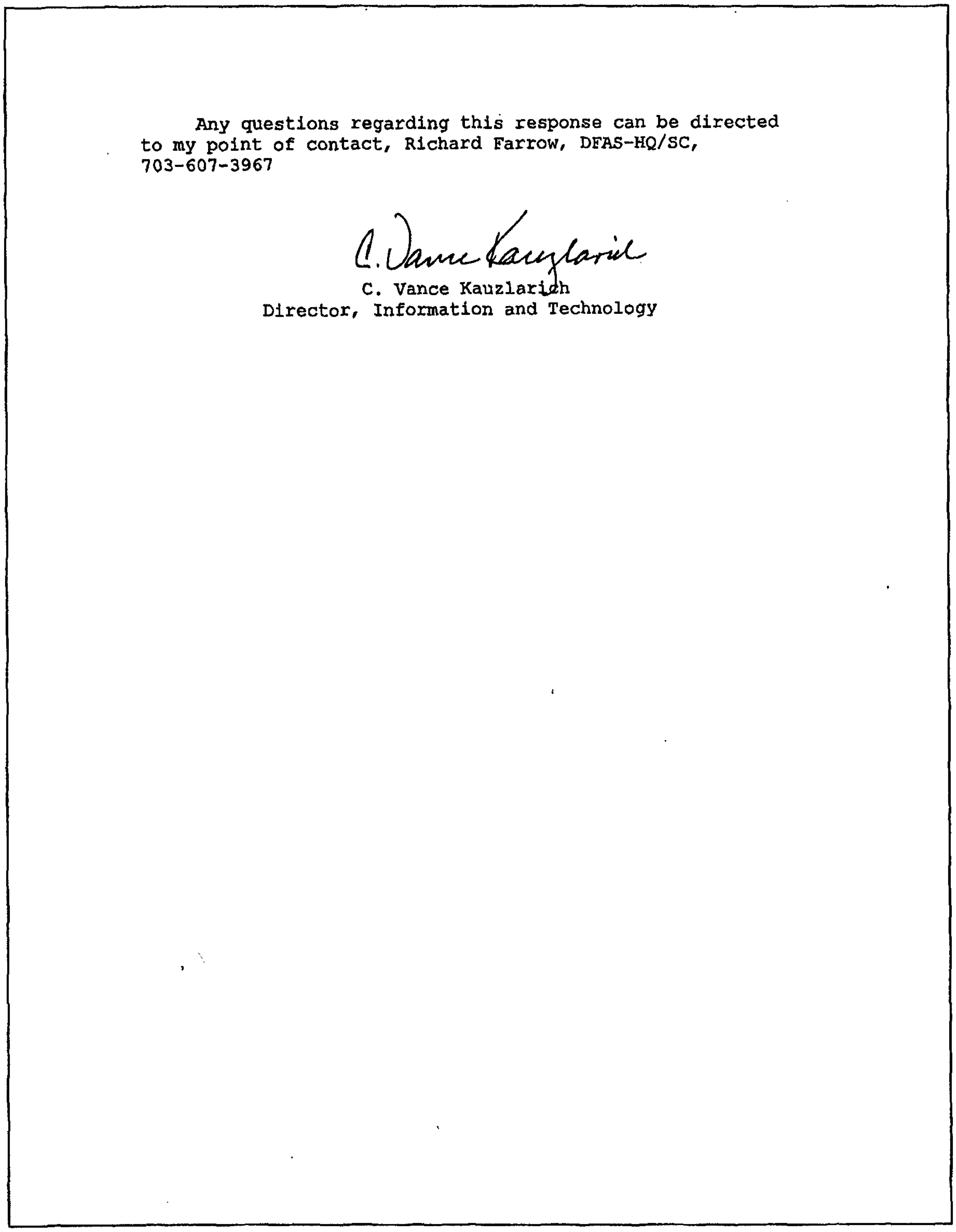
This memorandum is in response to the Department of Defense (DoD), Inspector General's (IG) initial findings after review of the Defense Finance and Accounting Service (DFAS) Center's cost reports for Year 2000.

DFAS concurs with the finding that initial cost estimates for finance systems were not complete. DFAS estimates did not always include all the necessary elements identified in the DoD Year 2000 Management Plan. DFAS recognized and acknowledged this shortcoming and has directed system managers to reassess their estimates to ensure all elements are addressed. In particular, system managers will verify that all functional costs (i.e., acceptance testing, contingency plan preparation) are included in their Year 2000 costs. Systems managers will continue to revisit their cost estimates, as their systems move toward reaching Year 2000 compliance.

Currently, DFAS' Year 2000 cost estimate is $39,987,000. This total includes both DFAS costs and non-DFAS costs for minority owned systems. The recent increase is due to re-evaluation of the original estimates and the inclusion of the elements that had originally been omitted.

DFAS will continue to fund Year 2000 costs from existing financial system budgets. If additional Year 2000 costs are identified, a reprioritization of the current workload will be executed to make the necessary funds available.

Appendix G. DFAS Memorandum on Y2K Cost Reporting



Any questions regarding this response can be directed to my point of contact, Richard Farrow, DFAS-HQ/SC, 703-607-3967

C. Vance Kauzlarich

C. Vance Kauzlarich
Director, Information and Technology

Appendix H. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Principal Deputy – Y2K
Assistant Secretary of Defense (Public Affairs)

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Chief Information Officer, Department of the Army
Inspector General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy
Chief Information Officer, Department of the Navy
Inspector General, Department of the Navy
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Chief Information Officer, Department of the Air Force
Inspector General, Department of the Air Force

Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
  Director for Information and Technology
Director, Defense Information Systems Agency
  United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

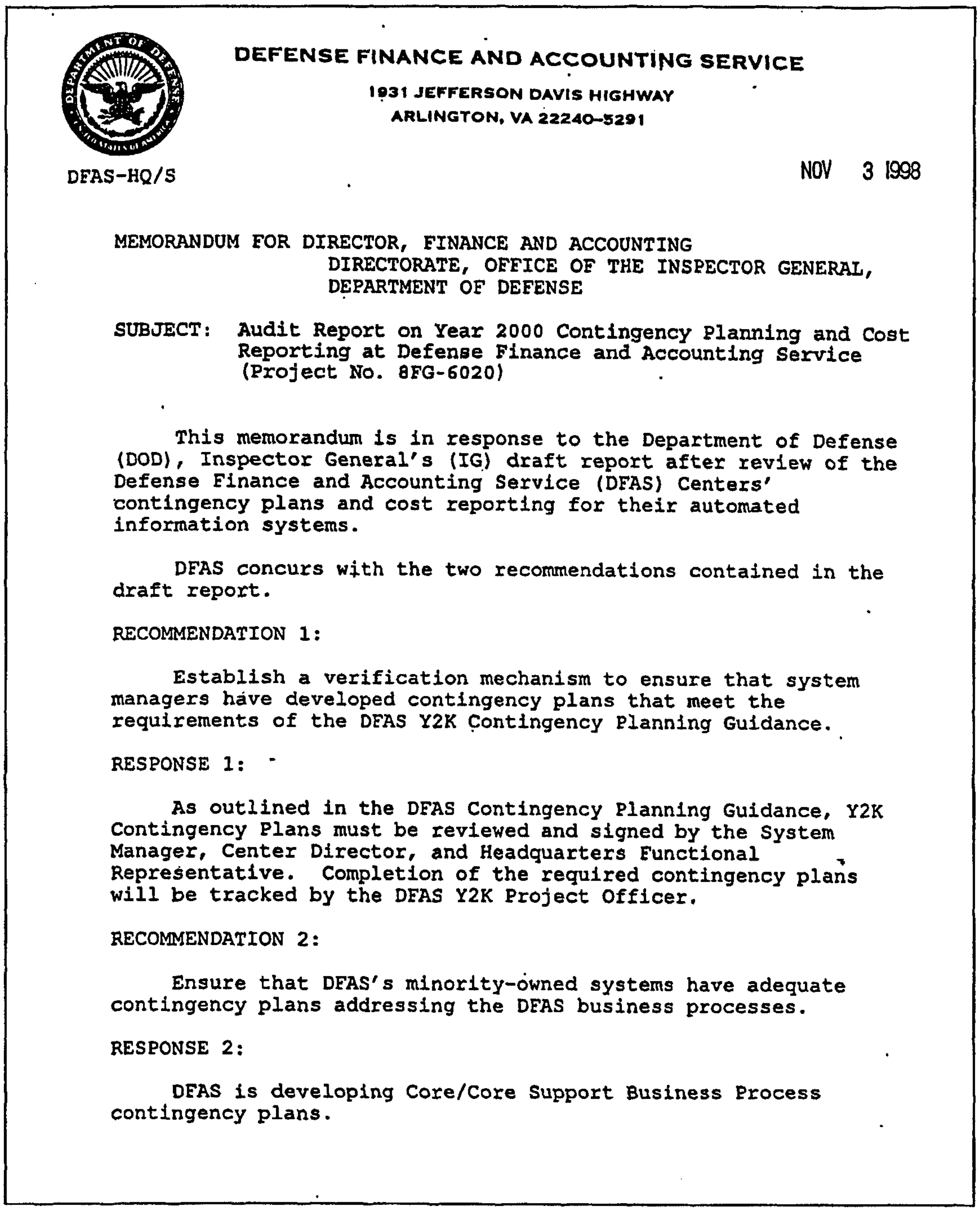
Office of Management and Budget
  Office of Information and Regulatory Affairs
Technical Information Center, National Security and International Affairs Division,
  General Accounting Office

Chairman and ranking minority member of each of the following congressional committees and subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Problem
House Committee on Appropriations
House Subcommittee on National Security, Committee on Appropriations
House Committee on Government Reform and Oversight
House Subcommittee on Government Management, Information, and Technology,
  Committee on Government Reform and Oversight
House Subcommittee on National Security, International Affairs, and Criminal Justice,
  Committee on Government Reform and Oversight
House Committee on National Security

Part III - Management Comments

Defense Finance and Accounting Service Comments



DEFENSE FINANCE AND ACCOUNTING SERVICE
1931 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22240-5291

DFAS-HQ/S

NOV 3 1998

MEMORANDUM FOR DIRECTOR, FINANCE AND ACCOUNTING
DIRECTORATE, OFFICE OF THE INSPECTOR GENERAL,
DEPARTMENT OF DEFENSE

SUBJECT: Audit Report on Year 2000 Contingency Planning and Cost Reporting at Defense Finance and Accounting Service (Project No. 8FG-6020)

This memorandum is in response to the Department of Defense (DOD), Inspector General's (IG) draft report after review of the Defense Finance and Accounting Service (DFAS) Centers' contingency plans and cost reporting for their automated information systems.

DFAS concurs with the two recommendations contained in the draft report.

RECOMMENDATION 1:

Establish a verification mechanism to ensure that system managers have developed contingency plans that meet the requirements of the DFAS Y2K Contingency Planning Guidance.

RESPONSE 1:

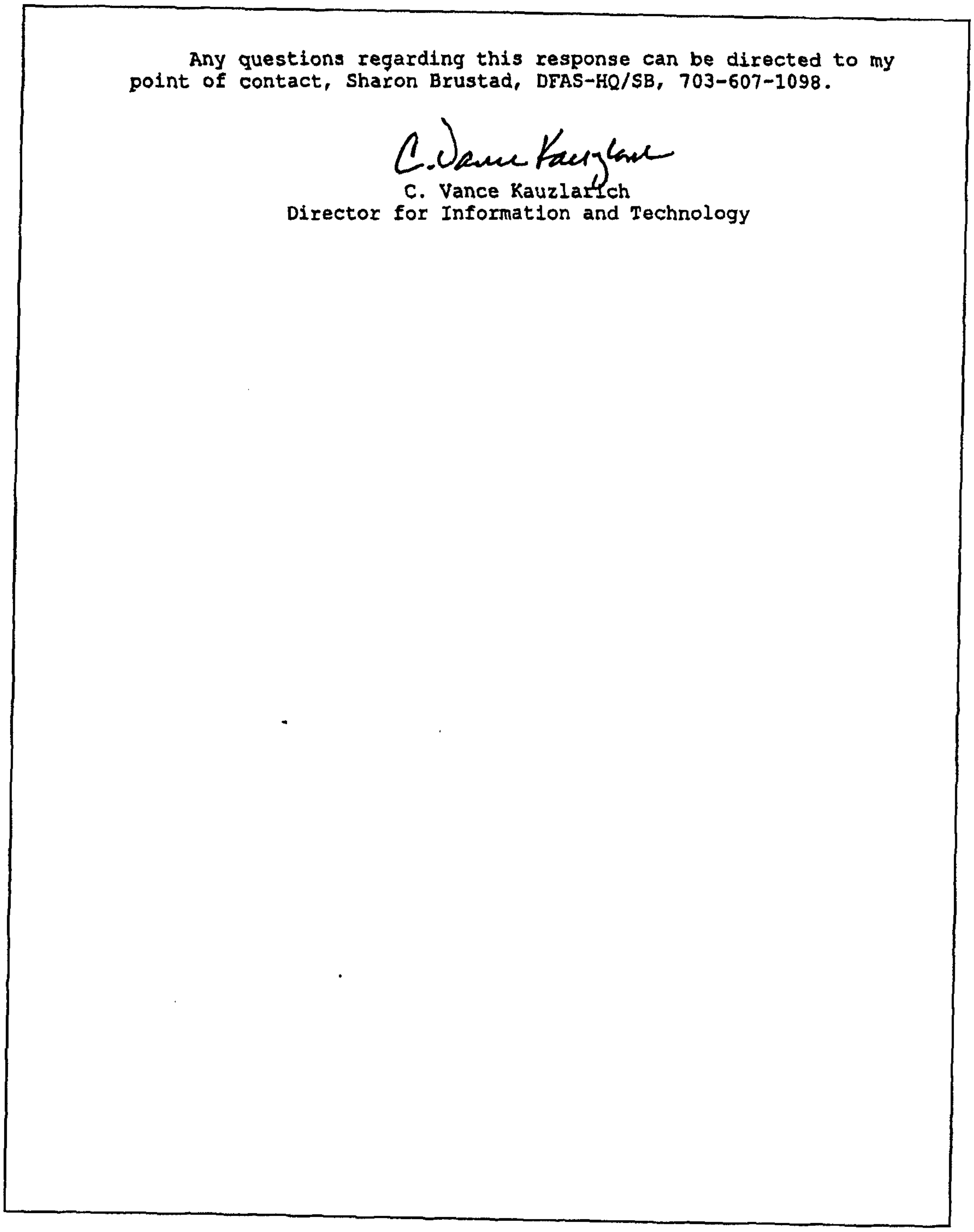
As outlined in the DFAS Contingency Planning Guidance, Y2K Contingency Plans must be reviewed and signed by the System Manager, Center Director, and Headquarters Functional Representative. Completion of the required contingency plans will be tracked by the DFAS Y2K Project Officer.

RECOMMENDATION 2:

Ensure that DFAS's minority-owned systems have adequate contingency plans addressing the DFAS business processes.

RESPONSE 2:

DFAS is developing Core/Core Support Business Process contingency plans.



Any questions regarding this response can be directed to my point of contact, Sharon Brustad, DFAS-HQ/SB, 703-607-1098.

C. Vance Kauzlarich
Director for Information and Technology

Audit Team Members

The Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report.

F. Jay Lane
Salvatore D. Guli
Kimberley A. Caprio
Michael Perkins
A. Dahnelle Alexander
Velma E. Garcia-White
William C. Coker
P. Douglas Johnston
Susanne B. Allen
Cheryl D. Jackson